

**IJCSIS Vol. 11 No. 4, April 2013**  
**ISSN 1947-5500**

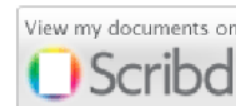
# **International Journal of Computer Science & Information Security**

**© IJCSIS PUBLICATION 2013**



Cogprints

Google scholar



SciRate.com

CiteSeer<sup>x</sup> beta



# IJCSIS

ISSN (online): 1947-5500

Please consider to contribute to and/or forward to the appropriate groups the following opportunity to submit and publish original scientific results.

## CALL FOR PAPERS

### International Journal of Computer Science and Information Security (IJCSIS) January-December 2013 Issues

The topics suggested by this issue can be discussed in term of concepts, surveys, state of the art, research, standards, implementations, running experiments, applications, and industrial case studies. Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.

See authors guide for manuscript preparation and submission guidelines.

**Indexed by Google Scholar, DBLP, CiteSeerX, Directory for Open Access Journal (DOAJ), Bielefeld Academic Search Engine (BASE), SCIRUS, Cornell University Library, ScientificCommons, EBSCO, ProQuest and more.**

**Deadline:** see web site

**Notification:** see web site

**Revision:** see web site

**Publication:** see web site

Context-aware systems  
Networking technologies  
Security in network, systems, and applications  
Evolutionary computation  
Industrial systems  
Evolutionary computation  
Autonomic and autonomous systems  
Bio-technologies  
Knowledge data systems  
Mobile and distance education  
Intelligent techniques, logics and systems  
Knowledge processing  
Information technologies  
Internet and web technologies  
Digital information processing  
Cognitive science and knowledge

Agent-based systems  
Mobility and multimedia systems  
Systems performance  
Networking and telecommunications  
Software development and deployment  
Knowledge virtualization  
Systems and networks on the chip  
Knowledge for global defense  
Information Systems [IS]  
IPv6 Today - Technology and deployment  
Modeling  
Software Engineering  
Optimization  
Complexity  
Natural Language Processing  
Speech Synthesis  
Data Mining

For more topics, please see web site <https://sites.google.com/site/ijcsis/>

 SCIRUS  
search engine for science

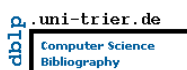
 ScientificCommons

 Scribd

 docstoc  
find and share professional documents

 BASE  
Bielefeld Academic Search Engine

 CiteSeerX beta

 dblp.uni-trier.de  
Computer Science  
Bibliography

 DOAJ  
DIRECTORY OF  
OPEN ACCESS  
JOURNALS

 EBSCO  
HOST

 ProQuest

For more information, please visit the journal website (<https://sites.google.com/site/ijcsis/>)

## Editorial

### Message from Managing Editor

**International Journal of Computer Science and Information Security (IJCSIS)** – established in 2009, has been at the forefront of new knowledge dissemination in research areas of computer science and applications, and advances in information security. The journal themes focus on innovative developments, research challenges/solutions in computer science and related technologies. IJCSIS aims to be a high quality publication platform and encourages young scholars and as well as senior academicians globally to share their research output and findings in the fields of computer science.

IJCSIS archives all publications in major academic/scientific databases; abstracting/indexing, editorial board and other important information are available online on homepage. IJCSIS editorial board consisting of international experts solicits your contribution to the journal with your research papers, projects, surveying works and industrial experiences. IJCSIS appreciates all the insights and advice from authors and reviewers. Indexed by the following International agencies and institutions: Google Scholar, Bielefeld Academic Search Engine (BASE), CiteSeerX, SCIRUS, Cornell's University Library EI, Scopus, DBLP, DOI, ProQuest, EBSCO. Google Scholar reported a large amount of cited papers published in IJCSIS. IJCSIS supports the Open Access policy of distribution of published manuscripts, ensuring "free availability on the public Internet, permitting any users to read, download, copy, distribute, print, search, or link to the full texts of [published] articles".

IJCSIS is currently accepting quality manuscripts for upcoming issues based on original qualitative or quantitative research that explore innovative conceptual framework or substantial literature review opening new areas of inquiry and investigation in Computer science. Case studies and works of literary analysis are also welcome.

We look forward to your collaboration. For further questions please do not hesitate to contact us at [ijcsiseditor@gmail.com](mailto:ijcsiseditor@gmail.com).

A complete list of journals can be found at:  
<http://sites.google.com/site/ijcsis/>

IJCSIS Vol. 11, No. 4, April 2013 Edition

ISSN 1947-5500 © IJCSIS, USA.

*Journal Indexed by (among others):*



## IJCSIS EDITORIAL BOARD

**Dr. Yong Li**

School of Electronic and Information Engineering, Beijing Jiaotong University,  
P. R. China

**Prof. Hamid Reza Naji**

Department of Computer Engineering, Shahid Beheshti University, Tehran, Iran

**Dr. Sanjay Jasola**

Professor and Dean, School of Information and Communication Technology,  
Gautam Buddha University

**Dr Riktesh Srivastava**

Assistant Professor, Information Systems, Skyline University College, University  
City of Sharjah, Sharjah, PO 1797, UAE

**Dr. Siddhivinayak Kulkarni**

University of Ballarat, Ballarat, Victoria, Australia

**Professor (Dr) Mokhtar Beldjehem**

Sainte-Anne University, Halifax, NS, Canada

**Dr. Alex Pappachen James (Research Fellow)**

Queensland Micro-nanotechnology center, Griffith University, Australia

**Dr. T. C. Manjunath**

HKBK College of Engg., Bangalore, India.

**Prof. Elboukhari Mohamed**

Department of Computer Science,  
University Mohammed First, Oujda, Morocco

IJCSIS  
2013

# TABLE OF CONTENTS

## **1. Paper 31031329: Security Policies for WFMS with Rich Business Logic — A Model Suitable for Analysis (pp. 1-9)**

*Fábio José Muneratti Ortega, Wilson Vicente Ruggiero*

*Departamento de Computação e Sistemas Digitais, Escola Politécnica da Universidade de São Paulo, São Paulo, Brazil*

*Abstract*—This paper introduces a formal metamodel for the specification of security policies for workflows in online service systems designed to be suitable for the modeling and analysis of complex business-related rules as well as traditional access control. A translation of the model into a colored Petri net is shown and an example of policy for an online banking system is described. By writing predicates for querying the resulting state- space of the Petri net, a connection between the formalized model and a higher-level description of the security policy can be made, indicating the feasibility of the intended method for validating such descriptions. Thanks to the independent nature among tasks related to different business services, represented by restrictions in the information flow within the metamodel, the state-space may be fractioned for analysis, avoiding the state-space explosion problem. Related existing models are discussed, pointing the gain in expressiveness of business rules and the analysis of insecure state paths rather than simply insecure states in the proposed model. The successful representation and analysis of the policy from the example combined with reasonings for the general case attest the adequacy of the proposed approach for its intended application.

*Keywords*-security policies; modeling and analysis; colored Petri nets; business workflows

## **2. Paper 31031337: A New Approach to Decoding of Rational Irreducible Goppa code (pp. 10-18)**

*Ahmed DRISSI*

*LabSiv : Laboratoire des Systèmes informatiques et Vision*

*ESCAM : Equipe de la Sécurité, Cryptographie, Contrôle d'Accès et Modélisation*

*Departments of Mathematics and Computer Science, Faculty of Sciences, Ibn Zohr University, Agadir, Morocco*

*Ahmed ASIMI*

*LabSiv : Laboratoire des Systèmes informatiques et Vision*

*ESCAM : Equipe de la Sécurité, Cryptographie, Contrôle d'Accès et Modélisation*

*Departments of Mathematics and Computer Science, Faculty of Sciences, Ibn Zohr University, Agadir, Morocco*

*Abstract* — The interesting properties of classical Goppa code and its effective decoding algorithm (algorithm of patterson) make the most appropriate candidate for use in the MC Eliece cryptosystem. Information leakage which results from the relationship between the error vector weight and the number of iterations in the decoding algorithm, presented a weakness of the cryptosystem. In this paper, we introduce a new approach to decoding, the use of binary Goppa code in system design MC Eliece which solve the problem of the leak of information, on the contrary in case of patterson algorithm. We treat this decoding method using the Newton identities and results of linear algebra.

*Keywords*: Binary Goppa code, the Newton identities, circulant matrix

## **3. Paper 21031305: RST-Based Analysis of Multi-Class Multi-Servers Non-Preemptive Priority Queues versus Worst Case IEEE Analysis (pp. 19-26)**

*(1) Amin B. A. Mustafa, (1) Mohammed A. A. Elmaleeh,*

*1 Faculty of Engineering, Alneelain University, Khartoum, Sudan, Jebra, Block16, No 433, Khartoum, Sudan.*

*Hassan Yousif (2), Mohammed Hussein (3),*

(2) College of Engineering, EE Dept, Salman bin Abdulaziz University, Wadi Aldwassir, KSA

(3) Faculty of Engineering, Sudan University of Science and Technology, Khartoum, Sudan

**Abstract**— In this paper, analysis of non-preemptive priority queues with multiple servers and multiple priority classes is presented. It is assumed that the service times – for all priority classes – are identically and exponentially distributed to simplify the complexity of the residual service time mathematical expression to an extent will enable calculating the average customer waiting time. The paper proposes an expression for the mean residual service time which then used in developing a mathematical model for the analysis of Pre-emptive and non-preemptive priority queues with multiple servers and multiple priority classes. This is followed by a comparative study between the proposed scheme and the Worst Case Analysis results. This could help a lot in justifying and supporting this proposed RSTBased Analysis.

**Keywords** - Non-preemptive; Multiple Servers; Mathematical Model

#### **4. Paper 22031311: Constructing Server-Clustering System with Web Services based on Linux (pp. 27-33)**

*Dr. Dhuha Basheer Abdullah Albazaz, Abdulnaser Yonis*

*Dept. of Computer Sciences, College of Mathematics and Computer sciences, University of Mosul- Iraq*

**Abstract** - This paper suggests a system that presents a high performance computing service across the internet. The system provides the ability of executing any parallel program by sending it from the client to be executed on the server. The ability of executing a wide range of programs is because of excluding the client-server system on only transferring files between client and server, while the responsibility of writing the source code, providing data, compiling and executing operations sequence are all assigned to the user and provided as input to the client side program. Web service technique is used in constructing the system for its high flexibility, and the ability of using it on different platforms. On the server side, translation and execution of parallel programs occurs by a Rocks cluster under the Linux-based CentOS operating system. Transferring files across the Internet was performed by using AXIOM objects that are included in Axis2 libraries.

**Keywords:** Cluster, web service, SOAP, Client, Server

#### **5. Paper 31031316: An Optimized Perona-Malik Anisotropic Diffusion Function for Denoising Medical Image (pp. 34-38)**

*A.S.M. Delowar Hossain*

*Assistant Professor, Dept. of CSE, Mawlana Bhashani Science and Technology University, MBSTU, Santosh, Tangail-1902 (Bangladesh)*

*Mehedi Hassan Talukder*

*Lecturer, Dept. of CSE, Mawlana Bhashani Science and Technology University, MBSTU, Santosh, Tangail-1902 (Bangladesh)*

*Md. Aminul Islam*

*Dept. of CSE, Mawlana Bhashani Science and Technology University, MBSTU, Santosh, Tangail-1902 (Bangladesh)*

*Md. Azmal Absar Dalim*

*Dept. of CSE, Mawlana Bhashani Science and Technology University, MBSTU, Santosh, Tangail-1902 (Bangladesh)*

**Abstract** — Noise is the major problem in the field of image processing. In Medical image such as Ultrasound image, MRI data and Radar Images are affected by different types of noise. So it is the most important task to eliminate such noises. In image processing anisotropic diffusion is a technique for reducing image noise without removing significant parts of the image contents, such as edges, lines or other details that are important to represent



the quality of the image. To acquire a better performance we state an another diffusion function that works efficiently to denoise an image without blurring the frontiers between different regions. To evaluate the performance we calculate the Signal to Noise Ratio, The Peak Signal to Noise Ratio, The Root Mean Square Error, The Edge Preservative Factor. This Function gives the better result with comparison to existing Perona-Malik anisotropic diffusion Function.

*Keywords- Anisotropic Diffusion, MRI data, Ultrasound Image, Speckle Noise, Gradient, Performance Evaluation.*

#### **6. Paper 31031318: New Paradigm for MANET Routing using Right Angled Biased Geographical Routing Technique (RABGR) (pp. 39-43)**

*Mr. V J Chakravarthy and Capt. Dr. S Santhosh Baboo*

*P.G. Research Dept of Com. Science, D. G. Vaishnav College, Arumbakkam, Chennai 600 106.*

*Abstract* — In this paper, we analyze the benefits of optimal multipath routing, to improve fairness and increase throughput in wireless networks with location information, in a bandwidth limited ad hoc network. In such environments the actions of each node can potentially impact the overall network connections. This is done by making multipath routing method, named as Right Angled Biased Geographical Routing (RABGR), and two congestion control algorithms, Biased Node Packet Scatter (BNPS) and Node-to-Node Packet Scatter (NNPS), which enhances the RABGR to avoid the congested areas of the network. The above RABGR method is used with AODV and AOMDV protocols and their results are compared. After Simulation, the experimental results shows that the solution achieve its objectives. Extensive ns-2 simulations show that the solution improves both fairness and throughput as compared to greedy routing using only single path.

*Keywords- MANET, AODV, AOMDV, Biased geographical routing, congestion, greeding routing.*

#### **7. Paper 21031301: Development of an Intelligent GIS Application for Spatial Data Analysis (pp. 44-49)**

*Pro. Dr. Hesham Ahmed Hassan, Dr. Mohamed Yehia Dahab, Eng. Hussein Elsayed Elsayed Abla*

*Cairo University*

*Abstract* - No one can deny Ambulance, Fire engine and police stations role in society service and feel all people safety and assurance, so we aim to get high performance and offer a good service through improve answer rate and Ambulance, Fire engine Centers and police stations distribution. Thus we integrated Geographic Information Systems (GIS) applications with domain expertise are saving time, effort and cost. The system aids the personnel to get critical spatial and non-spatial information. The system can identify the nearest Ambulance or Fire engine or police stations to the emergency location, and also determine the shortest route from the selected Ambulance station to the emergency location This framework is integrated GIS sciences can help users visualize map information and display spatial representations and suggestions for assessing existing Ambulance and Fire engine Centers performance hence planning and simulating for the future to approach for a good prediction and decision making with both static and dynamic spatial data.

*Keywords— Development of an Intelligent GIS application for spatial Data analysis; Emergency planning; Shortest route analysis; Decision making;*

#### **8. Paper 31031319: A New Technique to Accelerate Point Multiplication Specifically for a National Institute of Standards and Technology (NIST) recommended prime field p521 (pp. 50-54)**

*Anil kumar M. N, V. Sridhar*

*PET Research Foundation, PESCE, Mandya*

*Abstract* - In this paper we propose a new technique to accelerate point multiplication of NIST recommended prime field p521 when the point multiplication is computed by the instruction sets of general purpose microprocessors. We modified the Binary Inversion Algorithm used to compute the inversion which is the costliest operation among other arithmetic operations in point multiplication. Our modified Binary Inversion Algorithm reduces approximately



2,03,286.49 addition operations during a point multiplication when computed by binary scalar point multiplication algorithm. The effectiveness of the above method is analyzed by using statistical analysis. The analysis shows that our technique speeds up the inversion operation and consequently the scalar point multiplication of the NIST recommended prime field p521.

*Key words: Elliptic curve cryptography, Binary Inversion Algorithm, GF (p) arithmetic operators.*

#### **9. Paper 31031324: A Novel Agent based Communication in Wired-WIMAX Hybrid Network in MANET (pp. 55-61)**

*Kalyani Chaturvedi, M. TECH (EC. deptt.), Truba institute of engineering and information Technology, Bhopal, India*

*Neelesh Gupta, H.O.D. Dept. Of EC, Truba institute of engineering and information technology, Bhopal, India*

**Abstract** — Wireless technologies are able to provide mobility and portability that makes it more attractive as compared to wired technologies. Further, increasing requirement to support exiting connectivity with higher data rate for mobile computers and communication devices are performing a significant role to growing interest in wireless networks. WIMAX (Worldwide Interoperability for Microwave Access) is a telecommunications protocol that gives fixed and fully mobile internet access. This paper presents the role WIMAX technology in MANET at MAC layer. Wired network refers to interoperable implementations of the IEEE 802.3 and WIMAX which refers to interoperable implementations of the IEEE 802.16 wireless-networks standard. The radio range and data rate of WIMAX are much better then Wired network but, on the basis of cost WIMAX is expensive. In this paper is just proposal of a new hybrid network that is the communication between two different technologies on the basis of novel Agent, Wired Node (WN) and Mobile Node (MN). Now the Agent is worked as a interface in between wired and WIMAX network and Agent is connected with wired network to synchronize the communication with WIMAX, first the request is goes to Agent then to network. The combinations of these two technologies are not very expensive and also better than wired. In previous there is no such work done on Wired-WIMAX hybrid network. Their performance will be measure on the basis of TCP congestion window.

*Keywords- Wired Network, Agent, WN, MN, WIMAX, MAC, MANET, TCP.*

#### **10. Paper 31031325: Augmented Reality in ICT for Minimum Knowledge Loss (pp. 62-65)**

*Mr. RamKumar Lakshminarayanan, Dr. R D. Balaji, Dr. Binod kumar, Ms. Malathi Balaji  
Lecturer, Department of IT, Higher College of Technology, Muscat, Sultanate of Oman.*

**Abstract**—Informatics world digitizes the human beings, with the contribution made by all the industrial people. In the recent survey it is proved that people are not accustomed or they are not able to access the electronic devices to its extreme usage. Also people are more dependent to the technologies and their day-to-day activities are ruled by the same. In this paper we discuss on one of the advanced technology which will soon rule the world and make the people are more creative and at the same time hassle-free. This concept is introduced as 6th sense technology by an IIT, Mumbai student who is presently Ph.D., scholar in MIT, USA. Similar to this research there is one more research going on under the title Augmented Reality. This research makes a new association with the real world to digital world and allows us to share and manipulate the information directly with our mental thoughts. A college which implements state of the art technology for teaching and learning, Higher College of Technology, Muscat, (HCT) tries to identify the opportunities and limitations of implementing this augmented reality for teaching and learning. The research team of HCT, here, tries to give two scenarios in which augmented reality can fit in. Since this research is in the conceptual level we are trying to illustrate the history of this technology and how it can be adopted in the teaching environment.

*Keywords: Augmented Reality, 6th sense technology, Teaching and Learning, ICT*

#### **11. Paper 31031327: Optimizing Cost, Delay, Packet Loss and Network Load in AODV Routing Protocols (pp. 66-71)**

*Ashutosh Lanjewar, M.Tech (DC) Student, TIEIT (TRUBA), Bhopal (M.P), India*  
*Neelesh Gupta, Department of Electronics & Communication, TIEIT(TRUBA), Bhopal (M.P), India*

**Abstract:** AODV is Ad-hoc On-Demand Distance Vector. A mobile ad-hoc network is a self-configuring network of mobile devices connected by wireless. MANET does not have any fixed infrastructure. The device in a MANET is free to move in any direction and will form the connection as per the requirement of the network. Due to changing topology maintenance of factors like Packet loss, End to End Delay, Number of hops, delivery ratio and controlling the network load is of great challenge. This paper mainly concentrates on reducing the factors such as cost, End-to-End Delay, Network Load and Packet loss in AODV routing protocol. The NS-2 is used for the simulation purpose.

**Keywords:** AODV, Power consumption, End-to-End Delay, Network Load

## **12. Paper 31031346: Data Structures and Internet Application Identification (pp. 72-76)**

*Mrs. Mrudul Dixit*  
*Assistant Professor, Department of Electronics and Telecommunications, Cummins College of Engineering for Women, Karvenager, Pune – 411052, M.S. India.*

*Dr. Balaji V. Barbadekar*  
*Principal, Dyanganga College of Engineering, Pune, Maharashtra, India*

**Abstract —** Internet traffic describes the number of packets of various applications moving on the network. The internet traffic is increasing enormously day by day and so there is a need to monitor the network and the traffic for network management and planning, traffic modeling and detection, bandwidth analysis, etc. The identification of internet applications can be done on the basis of well known port numbers. The identification of application leads to analysis of bandwidth utilization by various internet applications. The port numbers are stored using different data structures. When a packet is received the port number from the packet is matched with the port numbers in the data structures. The time required to map is analyzed and should be minimum. The space required to store the database also should be minimum. There is always a tradeoff between the space and time. This paper deals with the analysis of space and time requirements for identification of internet applications based on well known port numbers using the data structures Binary Search Tree, AVL tree and Skip list. The packet capturing is done using tcpdump and Libpcap library on Linux platform using 'C' Language.

**Keywords-** Internet traffic, port number, skip list, AVL tree, BST.

## **13. Paper 31031347: Single MO-CFTA Based Current-Mode SITO Biquad Filter with Electronic Tuning (pp. 77-81)**

*S. V. Singh, Department of Electronics and Communication Engineering, Jaypee Institute of Information Technology, Sec-128, Noida, India*  
*R. S. Tomar, Department of Electronics Engineering, Anand Engineering College, Agra, India*  
*D. S. Chauhan, Department of Electrical Engineering, Institute of Technology, Banaras Hindu University, Varanasi-221005 (India)*

**Abstract —** This paper presents an electronically tunable current mode single input three output (SITO) biquad filter employing single multi-output current follower trans-conductance amplifiers (MO-CFTA). The proposed filter employs single resistor and two grounded capacitors. The proposed filter can simultaneously realize low pass (LP), band pass (BP) and high pass (HP) responses in current-mode. It is also capable of providing band reject (BR) and all pass (AP) responses without matching of components. In addition, the circuit possesses low sensitivity performance and low power consumption. The validity of proposed filter is verified through PSPICE simulations.

**Keywords-** component; CFTA, Biquad, Current-mode, Filter

## **14. Paper 31031348: Dynamic AODV for Mobile Ad-hoc Network (pp. 82-86)**

*Aditya Shrivastava, Information Technology, TIT, Bhopal, India*  
*Deepshikha Patel, Information Technology, TIT, Bhopal, India*  
*Amit Sinhal, Information Technology, TIT, Bhopal, India*

**Abstract** - Since long time work has been done to enhance working capability of AODV (Ad-hoc on demand distance vector routing protocol for Mobile Ad-hoc Network). Performance of AODV has been improved by some modification in its working procedure by many others researchers. Few parameters have been improved, and rest has been trade-offs. In this research work, AODV has been modified in such a way to improve its Dynamistic. Obviously, performance has been improved in terms of Throughput and Packet Delivery Ratio with the compromising Avg, End to End Delay and Routing/Network Overhead.

**Keywords:-** AODV, PDR, Networks Overhead, Throughputs, Avg. End-To-End Delay, Dynamic.

### **15. Paper 31031350: Steganography in Colored Images (pp. 87-92)**

*Iman Thannoon Sedeeq*  
*Department of Public Health, College of Veterinary Medicine, University of Mosul / Mosul, Iraq*

**Abstract** — Since people use internet daily they have to take care about information security requirement more and more. In this work a new algorithm for RGB based images steganography is presented. The algorithm uses LSB principle for hiding a variable number of secret message bits in RGB 24-bits color image carrier either in other one or two channels depending on the third one (index channel). The algorithm offered good capacity ratio with no visual distortion on the original image after hiding the secret message. Histograms of three channels (red, green, blue) are also compared before and after hiding process.

**Keywords-** Stganography; RGB; LSB; True color image.

### **16. Paper 31031355: Agent Behavior in Multiagent Systems: Issues and Challenges in Design, Development and Implementation (pp. 93-96)**

*Mohamed Ziyad TA, Lecturer in Dept. of CSE, SSM Polytechnic College, Tirur, Kerala, INDIA*  
*Dr KR Shankar Kumar, Professor in Dept. of ECE, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, INDIA*

**Abstract** — Multiagent System (MAS) technology, composed of multiple interacting intelligent agents, has become a new paradigm for modeling, designing, and implementing software solutions for complex and distributed problem solving. Multiagent system and its application have played an important part in academic research. The usages of agent based applications are increasing day by day with internet spreading widely. This study indent to address a brief area relating to the issues and challenges in the design, development and implementation of agent-based intelligent systems.

**Index Terms**—Distributed problem solving, intelligent agent, agent behavior,

### **17. Paper 31031357: A Comparative Study of VoIP Protocols (pp. 97-101)**

*Hadeel Saleh Haj Aliwi, Putra Sumari*  
*Multimedia Computing Research Group, School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia*

**Abstract** — Nowadays, Multimedia Communication has been developed and improved rapidly in order to enable users to communicate between each other over the Internet. In general, the multimedia communication consists of audio, video and instant messages communication. This paper surveys the functions and the privileges of different voice over Internet protocols (VoIP), such as InterAsterisk eXchange Protocol (IAX), Session Initiation Protocol (SIP), and H.323 protocol. As well as, this paper will make some comparisons among them in terms of signaling messages, codec's, transport protocols, and media transport, etc.

*Keywords- Multimedia; VoIP; InterAsterisk eXchange Protocol (IAX); Session Initiation Protocol (SIP); H.323 protocol; Signaling Messages*

**18. Paper 31011212: A Novel Approach for Object Detection and Tracking using IFL Algorithm (pp. 102-109)**

*R. Revathi, Research Scholar, Dept. of Computer Science, Karpagam University, Coimbatore, India  
M. Hemalatha, Dept. of Computer Science, Karpagam University, Coimbatore, India*

*Abstract* — This paper is an innovative attempt has been made using Attanassov's Intuitionistic fuzzy set theory for tracking moving objects in video. The main focus of this proposed work is taking an account for handling uncertainty in assignment of membership degree known as hesitation degree using Intuitionistic fuzzy. Many algorithms have been developed to reduce the computational complexity of movement vector evaluation. In this paper we propose to implement Intuitionistic logic based block Matching Algorithm termed as BMIFL to overcome the computational complexity. In this proposed methodology feature extraction is performed using 2Dfilter, segmentation using approximate median and object detection is done using our proposed algorithm Intuitionistic fuzzy. The results obtained clearly shows that our algorithm performs better than fuzzy logic based three Step Search algorithm.

*Keywords- component; Noise filtering, Segmentation, Object Tracking and detection, Fuzzy Logic.*

**19. Paper 31031326: A Comparative Study of some Biometric Security Technologies (pp. 110-120)**

*Ogini, Nicholas Oluwole  
Department of Mathematics and Computer Science, Delta State University, Abraka, Delta State*

*Abstract* - Authentication plays a very critical role in security related applications. This is obvious from the breaches of information systems recorded around the world. This has become a major challenge to ecommerce and many other applications. One of the techniques that is implemented today to improve information security is biometrics, and this is gaining attention as the days go by. Having realized its value, biometrics is used in most systems today for the verification and identification of users as it overcomes the problems of being stolen, borrowed, forged or forgetting. In this paper therefore, we show the origin and types of biometrics, their areas of application, and what to look out for in selecting a biometric technology.

**20. Paper 31031359: Digital Images Encryption in Spatial Domain Based on Singular Value Decomposition and Cellular Automata (pp. 121-125)**

*Ahmad Pahlavan Tafti, PhD Student, Department of Computer Science, University of Wisconsin Milwaukee  
Reyhaneh Maarefdoust, Sama technical and vocational training college, Islamic Azad University, Mashhad Branch, Mashhad, Iran*

*Abstract* — Protection of digital images from unauthorized access is the main purpose of this paper. A reliable approach to encrypt a digital image in spatial domain is presented here. Our algorithm is based on the singular value decomposition and one dimensional cellular automata. First, we calculate the singular value decomposition (SVD) of the original image in which the features of the image are extracted and then pushed them into the one dimensional cellular automata to generate the robust secret key for the image authentication. SVD is used as a strong mathematical tool to decompose a digital image into three orthogonal matrices and create features that are rotation invariant. We applied our proposed model on one hundred number of JPEG RGB images of size  $800 \times 800$ . The experimental results have illustrated the robustness, visual quality and reliability of our proposed algorithm.

*Keywords - Digital Images Encryption; Spatial Domain Encryption; Cellular Automata, SVD.*

## **21. Paper 31031356: Two-Level Approach for Web Information Retrieval (pp. 126-130)**

*S. Subatra Devi, PSVP Engineering College, Chennai, Tamil Nadu, India.*

*Dr. P. Sheik Abdul Khader, BSA Crescent Engineering College, Chennai, Tamil Nadu, India.*

*Abstract* - One of the most challenging issues for web search engines is finding high quality web pages or pages with high popularity for users. The growth of the Web is increasing day to day and retrieving the information, which is satisfied for the user has become a difficult task. The main goal of this paper is to retrieve more number of, most relevant pages. For which, an approach with two-levels are undergone. In the first level, the topic keywords are verified with the title of the document, the snippet, and the URL path. In the second level, the page content is verified. This algorithm produces efficient result which is being proved experimentally on different levels.

*Keywords* - *Information Retrieval; Crawler; Snippet.*

# Security Policies for WFMS with Rich Business Logic — A Model Suitable for Analysis

Fábio José Muneratti Ortega<sup>1</sup>, Wilson Vicente Ruggiero<sup>2</sup>

Departamento de Computação e Sistemas Digitais  
Escola Politécnica da Universidade de São Paulo  
São Paulo, Brazil

<sup>1</sup>fortega@larc.usp.br

<sup>2</sup>wilson@larc.usp.br

**Abstract**—This paper introduces a formal metamodel for the specification of security policies for workflows in online service systems designed to be suitable for the modeling and analysis of complex business-related rules as well as traditional access control. A translation of the model into a colored Petri net is shown and an example of policy for an online banking system is described. By writing predicates for querying the resulting state-space of the Petri net, a connection between the formalized model and a higher-level description of the security policy can be made, indicating the feasibility of the intended method for validating such descriptions. Thanks to the independent nature among tasks related to different business services, represented by restrictions in the information flow within the metamodel, the state-space may be fractioned for analysis, avoiding the state-space explosion problem. Related existing models are discussed, pointing the gain in expressiveness of business rules and the analysis of insecure state paths rather than simply insecure states in the proposed model. The successful representation and analysis of the policy from the example combined with reasonings for the general case attest the adequacy of the proposed approach for its intended application.

**Keywords**—security policies; modeling and analysis; colored Petri nets; business workflows

## I. INTRODUCTION

In spite of the many advances in security policies description, modeling and validation, designing secure systems under security constraints involving business parameters can lead to large models that are unsuitable for analysis. Additionally, descriptions of security policies based on entities with a high level of abstraction result in models distant from the system's implementation, potentially leading to the inclusion of vulnerabilities in the translation or, if methodically or automatically translated, may still lead to inefficient software.

Our objective is to define a modeling and analysis strategy that best suits the validation of security policies meant primarily for online services systems and that properly handles rules heavily dependent of workflow states and business parameters.

We begin by situating the problem from a communication-based view of a workflow system. Next, the metamodel developed is defined and its notable features discussed, and finally, the process of analysis is considered leading to the

comparison with other approaches and the conclusions on the adequacy of the process.

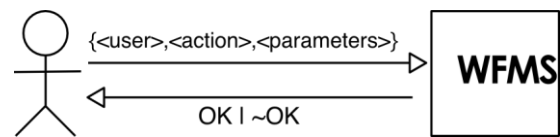


Figure 1. Model of communication with the WFMS.

## II. DESCRIBING WORKFLOWS

The use of Petri nets (PN) [1] for modeling business workflows has been widely accepted for years, mainly thanks to their mathematically sound nature combined with their large power of representation of state-based scenarios [2]. The extended concept of colored Petri nets (CPN) [3] enhances the expressiveness of models and simplifies their analysis, especially when aided by tools such as the CPN Tools software [4]. In [5] these characteristics of PN have been exploited as the authors devised the possibility of linking workflows to multilevel secure environments, thus treating problems of authorization within such workflows as reachability problems in their corresponding modeled Petri net [6]. This approach makes it possible to formally analyze whether a security policy is respected in a given scenario.

Regardless of its structure, a workflow management system (WFMS) may be seen, from its inputs and outputs point of view, as an entity receiving sequences of messages, or *requests*, from the interacting parties that alter its inner state. For the specification of a security policy for such a system, the most important feature is whether or not it authorizes each received request.

Figure 1 indicates the structure of a request. The interacting party that issues the request will be referred to as *user*. Each request specifies a desired *action*, which is subject to security constraints. The set of actions related to the same high-level business process form a *task*. The *parameters* specify the scope of the action, and may be thought of as lists of key-value pairs.

By restricting the mathematical domains for those parts of a request, one may define the set of possible sequences of

requests for performing tasks that we shall call *protocol* of the WFMS. Therefore, the description of the sequences of messages that lead to authorized or forbidden actions constitute a formal language, which we'll refer to as the high-level description of the policy in the context of our model.

Based on these formulations, our strategy for validating security policies for WFMS is:

- 1) Determine the protocol for a given system;
- 2) Describe the security policy in terms of the authorized and unauthorized sequences of requests;
- 3) Model the security policy in terms of a special metamodel; and
- 4) Translate the high-level description of the policy into predicates that query such metamodel's state-space for validating that it fully represents the described security policy.

This paper discusses the design of this metamodel, that must be capable of modeling complex security rules related to business parameters and must also feature an architecture that facilitates the analysis of the models. The analysis suggested in the last step of the strategy defined above is not a complete one. It is enough to demonstrate that models designed in terms of this metamodel properly represent the security policies they were meant to represent, and that the model's architecture supports analyses based on querying its state-space. Additionally, since the metamodel models a complete and consistent set of rules by design, inconsistencies in the rules that guide the query-based analysis will be discovered. However, demonstrating the completeness of this set of rules would require other verifications that although haven't been shown in the scope of this work, also rely on observing aspects of the state-space and can be achieved with no changes to the metamodel.

We focus on verifying that: (a) the metamodel conceived is capable of representing the security policies of the desired scenario without compromising the feasibility of the analysis, and (b) there is a method for translating the typical sequences of messages that will define rules in WFMS into queries that may be designed in the realization of the model using CPN Tools.

#### A. Example: Policy For Online Banking System

We demonstrate the ideas proposed with the help of an example of security policy meant for regulating the clients' access to an online banking system. The financial services selected for the example are a simple balance check and an electronic funds transfer (EFT) operation. These two, along with the login and logout operations suffice to demonstrate the methodology to be followed and the power and limitations of the modeling.

In this example, each bank account holds two users, one called "master" and another called "helper". Users authenticate via a login procedure where only a password is provided for the sake of simplicity. The balance check is a

simple read-only transaction whereas the EFT requires more complex rules that demonstrate how to represent business-specific scenarios.

The protocol for the example is given below (arrows indicate workflow sequence):

##### Login

Actions: "idtf" (acc, usr) → "auth" (pass)

"idtf" Identifies the account and user for logging in. "auth" sends the password for the (user, account) pair.

##### Balance

Actions: "balance"

A single message for requesting balance, dependent on the login.

##### ETF

Actions: "transf\_home" → "transf\_forms" (acc, val) → "transf\_auth" (idt, pass)

"transf\_home" represents the request for a funds transfer page containing the required forms. "transf\_forms" represents the sending of those forms including account to receive funds and value. "transf\_auth" represents the sending of the necessary credentials for confirming the operation.

The rules of the policy are as follows:

- 1) For a *login*, the requesting user must not have completed a login before under the requested account, unless it has completed a logout in between them.
- 2) Failing to provide the correct password to the *login* on three consecutive occasions blocks the access to the system.
- 3) Only logged users may access the account *balance*.
- 4) Only logged users may access the *electronic funds transfer* operation.
- 5) Only the "master" user may complete electronic funds transfer operation; the "helper" user may only format them for later approval.
- 6) The amount to *transfer* to a non-registered account added to the total amount already transferred to non-registered accounts must not exceed the limit of \$500.
- 7) The amount to *transfer* to a registered account added to the total amount already transferred must not exceed the limit of \$1500.

Each of these may be specified in terms of authorized and denied sequences of messages, as will be discussed in the analysis of the example. A small CPN implements the sending of sequences of messages to the metamodel, optionally regulating stop criteria.

### III. THE METAMODEL

The metamodel must provide an abstraction for the inner state of the WFMS as well as include the mechanisms by means of which a modeled policy shall define the logic of authorization of workflows and evolution of the inner state abstraction.



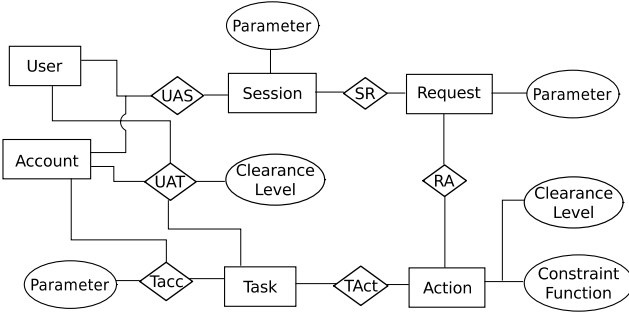


Figure 2. Entity-relationship diagram for the metamodel.

For defining the inner state model, some assumptions on the type of system under discussion are pertinent. Unlike many workflow systems in the literature, online services systems are marked by a wide range of possible operations, or *tasks*, and limited shared resources. In the context of the metamodel, the *account* will act as the only shared resource repository. That'll prove not to be too limiting, since an unlimited number of parameters may be modeled as resources in each account.

Figure 2 presents the metamodel as an entity-relationship model. A *user*, accessing an *account*, initiates a *session*. By means of this session, the requests are issued. Every account holds parameters relative to each performable task. There are also specific parameters for each session and each request. Every triple (user, account, task) is assigned a certain clearance level, and each possible action is associated with a minimum clearance level needed for its authorization. Besides that, every action is also assigned a constraint function that holds the authorization logic for that action in terms of the requesting entities and their parameters. The definitions concerning a security policy modeled on top of this metamodel should, therefore, be achieved by providing values to the depicted attributes — parameters, clearance levels and constraint functions. Taking its formal interpretation as explained in [7], the formal definition of the metamodel follows.

**Definition 1:**

- Let User, Account, Session, Request, Action and Task be entity sets;
- Let  $UAS \subseteq User \times Account \times Session$  be a relation assigning a session to a user and account;
- Let  $UAT \subseteq User \times Account \times Task$  be a relation assigning a task to a user and account;
- Let  $SR \subseteq Session \times Request$  be a relation assigning a request to a session;
- Let  $RA \subseteq Request \times Action$  be a relation assigning an action to a request;
- Let  $Tact \subseteq Task \times Action$  be a relation assigning an action to a task;

- Let  $TAcc \subseteq Task \times Account$  be a relation assigning an account to a task;
- Let Key, Value, Clearance, Integer and String be value sets, with  $Key \subseteq String$ ,  $Clearance \subseteq Integer$  and  $Value \subseteq Integer \cup String \cup 2^{Integer} \cup 2^{String}$ ;
- Let  $Parameter \subseteq Key \times Value$  be a relation assigning a value to a key;
- Let  $P_S: Session \rightarrow 2^{Parameter}$  be a function that represents a session's *Parameters* attribute by mapping a Session to a set of Parameter (to be defined in the metamodel implementation);
- Likewise, let  $P_R: Request \rightarrow 2^{Parameter}$  and  $P_{TA}: TAcc \rightarrow 2^{Parameter}$  be functions representing the analogue attributes; and
- Let  $Cl_A: Action \rightarrow Clearance$  and  $Cl_{UAT}: UAT \rightarrow Clearance$  be functions representing the *Clearance Level* attributes;

Given the above definitions, one may formalize the authorization of a request:

**Definition 2:**

- Let  $\geq_{Cl} \subseteq Clearance \times Clearance$  be a partial order on the set of Clearances;
- Let  $C_A: Action \rightarrow (2^{Parameter} \times 2^{Parameter} \times 2^{Parameter} \times User \times Account \rightarrow \{true, false\})$  be a higher-order function mapping an Action to a Boolean-valued *constraint function* (referenced ahead as  $f_A$ );
- Let  $\psi(r): Request \rightarrow \{true, false\}$  be an auxiliary predicate such that:

$$\psi(r) := \{ Cl_{UAT}(uat) \geq_{Cl} Cl_A(a) \mid \exists a \in Action : RA(r, a) \wedge \exists s \in Session : SR(s, r) \wedge \exists u \in User, acc \in Account : UAS(u, acc, s) \wedge \exists t \in Task : TAct(t, a) \wedge \exists uat = (u, acc, t) : UAT(uat) \}$$

and

- Let  $\phi(r): Request \rightarrow \{true, false\}$  be a predicate such that:

$$\phi(r) := \{ C_A(act) (P_R(r), P_{TA}(\tau), P_S(s), u, acc) \wedge \psi(r) \mid \exists act \in Action : RA(r, act) \wedge \exists s \in Session : SR(s, r) \wedge \exists u \in User, acc \in Account : UAS(u, acc, s) \wedge \exists t \in Task : TAct(t, act) \wedge \exists \tau = (t, acc) : TAcc(\tau) \}$$

Then, a request  $r$  is said to be authorized if, and only if, it satisfies the predicate  $\phi(r)$ .

Predicate  $\psi(r)$  is the authorization stage that implements multilevel access control by checking whether a certain user working with a certain account has enough clearance for performing its desired action in the context of that specific task.

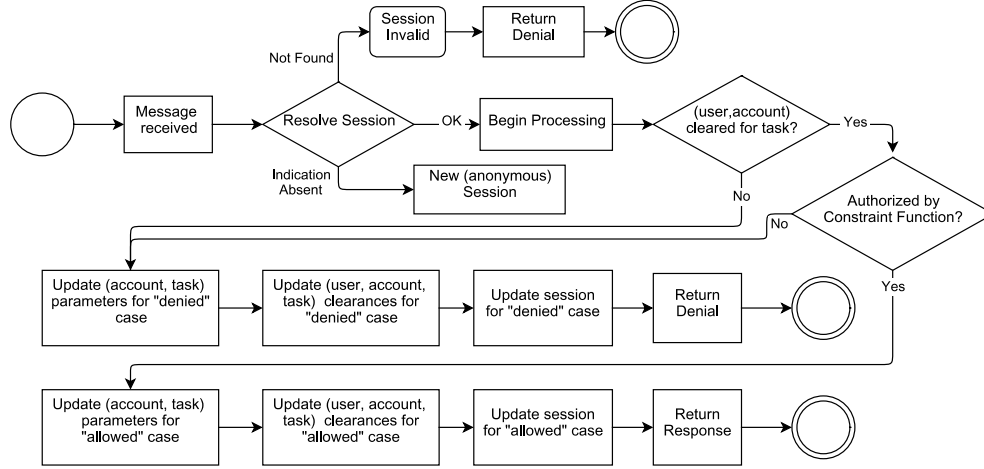


Figure 3. Stages of the processing of a request.

The constraint functions  $f_A$ , defined for each action in the model, is the placeholder for any complex business logic to be included in a security rule. In a strict view,  $f_A$  is capable of including the functionality that  $\psi(r)$  provides, but having a separate mechanism for multilevel access control simplifies the modeling given its frequent usage.

Besides the authorization stage, a *state update* stage is desired, as represented by the flowchart in figure 3. By including updates to the model's attributes, decisions regarding the authorization of subsequent requests may differ from previous ones, effectively making the model dynamic. There are three updates contemplated by the metamodel: update of the (account, task) parameters, update of the (user, account, task) clearances and update of the session as a whole (entities, relations and parameters). Adopting a superscript  $\Delta$  as notation for values during the processing of a request  $r$  and  $\Delta + 1$  for their updated values during processing of the request that follows  $r$ , the update rules are formally defined as follows:

**Definition 3:** Let  $A_P: \text{Task} \times 2^{\text{Parameter}}$ , then we define the *account parameters update function*  $f_B$ :

$$f_B: 2^{\text{Parameter}} \times 2^{A_P} \times 2^{\text{Parameter}} \times \text{User} \times \text{Account} \times \text{Task} \rightarrow 2^{\text{Parameter}}$$

And so, for the account  $acc$  processed in  $\Delta$  and  $\forall t \in \text{Task}$ :

$$P_{TA}^{\Delta+1}(t, acc) = f_B(P_R(r), \bigcup_{\tau \in \text{Task}} (\tau, P_{TA}^{\Delta}(\tau, acc)), P_S^{\Delta}(s), u, acc, t)$$

where  $r$  is the request processed in  $\Delta$ ,  $s \in \text{Session} : \text{SR}(s, r)$  and  $u \in \text{User} : \text{UAS}(u, acc, s)$ .

For any other  $acc' \in \text{Account}$ ,  $\forall t, P_{TA}^{\Delta+1}(t, acc') = P_{TA}^{\Delta}(t, acc')$ .

This means that only parameters relative to the account that issued the request may be updated, however parameters from different tasks than the one processed may also suffer changes, therefore allowing some dependence between tasks in the security policy design.

For the update of (user, account) clearances, we define:

**Definition 4:** Let  $UA_C: \text{Task} \times \text{Clearance}$ , then we define the *clearances update function*  $f_C$ :

$$f_C: 2^{\text{Parameter}} \times 2^{\text{Parameter}} \times 2^{\text{Parameter}} \times 2^{UA_C} \times \text{User} \times \text{Account} \times \text{Task} \rightarrow \text{Clearance}$$

and so, for entities related to the processed request in the same terms as in the previous definition,  $\forall t \in \text{Task}$ :

$$Cl_{UAT}^{\Delta+1}(u, acc, t) = f_C(P_R(r), P_{TA}^{\Delta}(t, acc), P_S^{\Delta}(s), \bigcup_{\tau \in \text{Task}} (\tau, Cl_{UAT}^{\Delta}(u, acc, \tau)), u, acc, t)$$

For any other  $acc' \in \text{Account}$ ,  $u' \in \text{User}$ ,  $\forall t$

$$Cl_{UAT}^{\Delta+1}(u', acc', t) = Cl_{UAT}^{\Delta}(u', acc', t).$$

Thus, analogously as with  $f_B$ , a policy may alter the clearances for any task, but only for the pair (user, account) that issued the request. Finally, for updating the session related elements:

**Definition 5:** We define the *session update function*  $f_D$ :

$$f_D: 2^{\text{Parameter}} \times 2^{\text{Parameter}} \times 2^{\text{Parameter}} \times \text{User} \times \text{Account} \times \text{Session} \rightarrow 2^{\text{Session}} \times 2^{SR} \times 2^{\text{Parameter}}$$

And so, for entities related to the processed request,

$$(\text{Session}^{\Delta+1}, SR^{\Delta+1}, P_S^{\Delta+1}) = f_D(P_R(r), P_{TA}^{\Delta}(t, acc), P_S^{\Delta}(s), u, acc, s).$$

Each of the function kinds  $f_B$ ,  $f_C$  and  $f_D$  must have a definition in the metamodel implementation for appliance following *authorized* requests and another for appliance following *denied* requests, as denoted in the flowchart.

As a final remark, one may notice that security policies defined according to this metamodel will be inherently *consistent*, since only a single function for each purpose — authorization or state updates — may be defined for each action defined in the protocol; *complete*, and *non-redundant*,

since the logic of authorization is bound to all possible interactions with the system, instead of to rules encompassing sets of interactions, which could leave gaps (incompleteness) or overlap (redundancy). However, precisely for not being a rule-oriented design, the modeled policy must be proven equivalent to our high-level specification, which is the purpose of the analysis.

#### A. The CPN Model

The translation of the conceptual metamodel conceived into a CPN model is rather straightforward.

Figure 4 shows the network that implements the metamodel. The central transition tagged “execution” handles the entire process seen in the flowchart from figure 3. The input requests are withdrawn from a queue implemented in the place called “server queue” and responses are sent to another queue in the place “server output”. Session identifications are generated in the place “new session pool”, and the identification number is consumed only in case a new session is processed. The smaller transition, tagged “session invalid” is triggered only in case a certain session identification received is not found in the open sessions pool, located in the place named “open sessions”. That mechanism for the invalid sessions is achieved using a lower priority for the firing of that transition. The tokens stored in the place “open sessions” include four pieces of information: the identification of the session, the user associated with it, the account also associated with it and the parameters of the session. The remaining places, “account data access” and “user data access” hold the parameters linked to each account for every task and the (user, account, task) clearance levels, respectively. The guard function for the execution transition ensures that the selected session corresponds to the one referenced by the parameter with key equal to “sess” in the request, when it is present. The code region for the same transition distinguishes new sessions from sessions retrieved from the “open sessions” place and executes the authorization function determining the decision for the request in process. The authorization function is responsible for both stages defined in the flowchart — the first one,  $\psi(r)$ , referencing the clearance required for the action, and the second one referencing the constraint function for the action. Finally, the output arcs take care of the update of each entity by calling an execution function which references all the right functions defined in the policy, using the result of the authorization function to determine whether to invoke functions for denial or allowance of execution. The output arc leading to the output queue calls a function that assembles the reply message, also for denial or allowance accordingly.

#### B. Implementing the Example Policy

As had been explained in the introduction of the metamodel, the security policy is entirely described for the model by establishing the values for all attributes from the entity- relationship model provided. Table I shows a simplified view of that description as it is implemented for the rules above.

TABLE I. SUMMARY OF MODELED POLICY

Action	Task	Clearance	$f_A$	$f_B$	$f_C$	$f_D$
idtf	login	0	X		X	X
auth	login	0	X	X	X	
balance	balance	1	X			
transf_home	eft	1	X			X
transf_forms	eft	1	X	X		X
transf_auth	eft	2	X	X		
logout	logout	0		X	X	X

The “Clearance” column indicates the clearance level required for the pair (user, account) to perform the action required by the request. All pairs initiate runs of the Petri net with value 0 (zero), gaining higher clearance levels as they log in or perform other actions. The function  $f_A$  is the constraint function that determines whether or not the action may be completed. In the table, cells marked with an “X” indicate that the evaluation of a function of the type given by that column is necessary for actions of the type indicated in the row. For functions  $f_B$  (account parameters update),  $f_C$  (clearances update) and  $f_D$  (session update), an empty cell indicates that for that action, an identity function is used for that feature, which means no change is necessary for that entity. The indication of functions for updates in case of denial of intent are omitted to avoid cluttering, but they shall be necessary at most for the same cases as their allowed update counterparts.

It can be noted from table I that, for instance, the “idtf” action requires a constraint function, a clearance update function and a session update function, but doesn’t require an account parameters update function. Indeed, the clearance update function is needed because the clearance for all other tasks is reduced below zero, since the session is about to become associated to a user and account that haven’t been validated yet. The session update function is needed to indicate which user and account the session is attempting to impersonate. The constraint function is necessary to verify if a free session identifier for allocation, and finally the account parameters shouldn’t be updated, since at this point it is yet unknown whether the user actually has access to the account it claims to have (the limitation of the model of only being able to update the account associated to the running session prevents updates on any valid accounts at this point, since there is no account linked to the session until that very update that  $f_D$  from “idtf” intends to execute). A sample of an authorization function ( $f_A$ ) for the “transf\_auth” action is given below:

```
fun transf_auth_funA (m:request, s:session, q:params) =  
let  
  val password = StringInParam(getOpt(valueForKey  
    ("u"^(toString(usrNumber(#3 s)))) (q),ValString(""))))  
  val registered = IntListInParam(getOpt(  
    valueForKey "registered" (q), ValIntList([])))  
  val avLimit = IntInParam(getOpt(  
    valueForKey "avLimit" (q), ValInt(50000)))  
  val avLimitRegistered = IntInParam(getOpt(  
    valueForKey "avLimitReg" (q), ValInt(150000)))  
  val tid = IntInParam(getOpt(  
    valueForKey "tid" (#3 m), ValInt(~1)))  
  val destAcc = AccInParam(getOpt(valueForKey
```

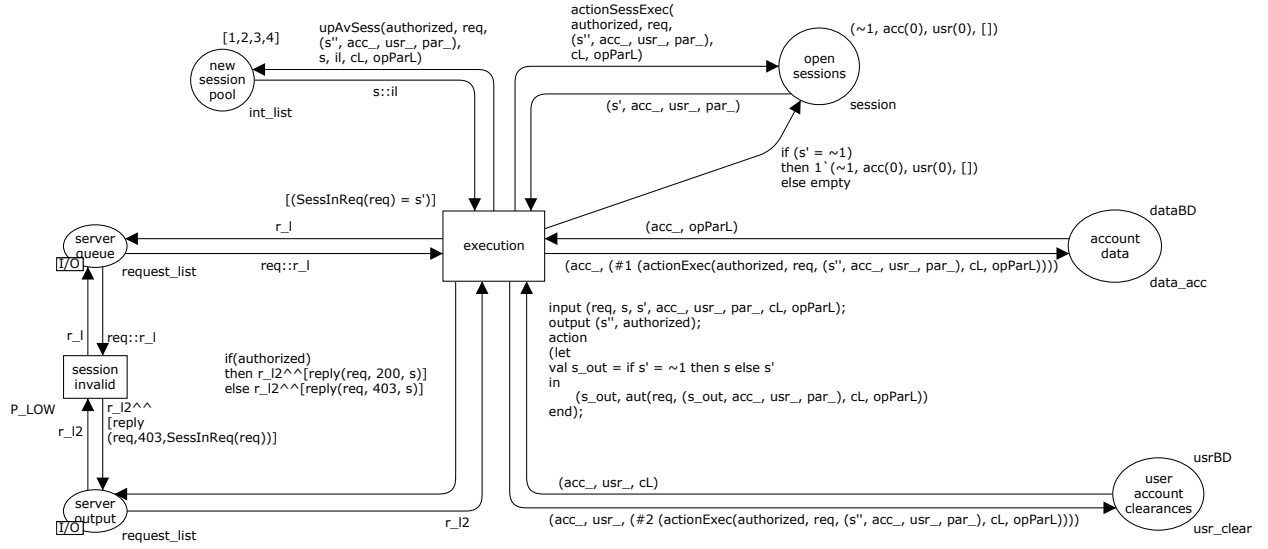


Figure 4. The colored Petri net for the metamodel

```

(("tr"^(toString(tid)))^"_to") (q), ValAcc(acc(0)))
val value_ = IntInParam(getOpt(valueForKey
  ("tr"^(toString(tid)))^"_val") (q), ValInt(~1)))
in
  value_ > 0
andalso
  destAcc <> acc(0)
andalso
  destAcc <> (#2 s)
andalso
  if (mem registered (accNumber(destAcc)))
  then avLimitRegistered + avLimit >= value_
  else avLimit >= value_
andalso
  StringInParam(getOpt(valueForKey "auth" (#3 m),
    ValString("")) = password
andalso
  sessOK(m, s, q)
end;

```

The function's input matches the definition for constraint functions: the value  $m$  holds the request parameters,  $q$  holds the parameters for the pair (account, task) and  $s$  is a triple containing user, account and session parameters. The auxiliary values `password`, `registered`, `avLimit` and `soforth` are all extracted from the account parameters for the EFT task ( $q$ ) except for `tid` which is a parameter from the request. `tid` identifies the EFT previously prepared for execution, and, therefore, its parameters of value and recipient account are located by referencing it. Default values are specified for all parameters in case they aren't found. The authorization is granted given that the transaction value is larger than zero, the recipient account is valid and isn't the session's own account, the password provided in the request matches the saved password for that user in the account's parameters, and the account's limits are greater than the transaction value, with the appropriate limit calculated depending on whether the recipient account is registered or not. This sample fully demonstrates the complexity that can be achieved in the semantics of the rules thanks to the minimal restrictions provided by the metamodel.

## IV. MODEL ANALYSIS

### A. Defining Rules Precisely

The main goal of the metamodel analysis as we have conducted it is demonstrating that it fully represents the security policy described by means of accepted and rejected sequences of requests. In order to indicate these sequences and define rules precisely, a notation is introduced. The expression below indicates rule (1) from the example written using such notation:

$$(u, a) \text{ "auth" } (sess = s)()^A \rightarrow \neg((u, a) \text{ "logout" } (sess = s)()^A) \Rightarrow (u, a) \text{ "idtf" } (acc = a, usr = u)^D$$

$\alpha \Rightarrow R^\delta$  means that if conditions  $\alpha$  are respected, decision  $\delta$  must be applied to request  $R$ .  $R^D$  indicates the denial of  $R$ .  $R^A$  indicates the authorization of  $R$ . Operator " $Q \rightarrow R$ " indicates  $R$  has been processed after  $Q$  (not necessarily *immediately* after). Operator  $\neg R$  indicates  $R$  has not been processed. The first pair of parentheses after each action name encloses request parameters and the second, response parameters (hence, there is no second pair of parentheses for the request under analysis). Thus, the rule reads: "Requests from user  $u$  for action *idtf* on account  $a$  shall be denied if there has been a previous authorized processing of an action *auth* for the same user and account in a session  $s$  that hasn't been followed by an authorized request for action *logout*, also in session  $s$ ."

It is not our purpose to formalize this notation in this paper. We employ it simply as an intermediate step for designing predicates over state-the space that capture the semantics of the rules written in natural language.

And so, for the remaining rules from the given example of policy:

$$\begin{aligned}
 2) \quad & (u, a) \text{ "auth" } ()()^D \rightarrow \neg((u, a) \text{ "auth" } ()()^A) \rightarrow \\
 & (u, a) \text{ "auth" } ()()^D \rightarrow \neg((u, a) \text{ "auth" } ()()^A) \rightarrow \\
 & (u, a) \text{ "auth" } ()()^D \Rightarrow (u, a) \text{ " " } ()^D
 \end{aligned}$$

- 3)  $\neg((u, a) \text{“auth”}(\text{sess} = s)()^A) \Rightarrow (u, a) \text{“balance”}(\text{sess} = s)^D$
- 4)  $\neg((u, a) \text{“auth”}(\text{sess} = s)()^A) \Rightarrow (u, a) \text{“transf\_home”}(\text{sess} = s)^D$
- 5)  $(u, a) \text{“transf\_auth”}()^D, u = \text{“helper”}$
- 6)  $[(u, b) \text{“transf\_forms”}(\text{val} = v, \text{dest} = a)(\text{id} = t)^A \rightarrow (u, b) \text{“transf\_auth”}(\text{id} = t)^A]^I \rightarrow (u, b) \text{“transf\_forms”}(\text{val} = v_k, \text{dest} = a_k)(\text{id} = t_k)^A \Rightarrow (u, b) \text{“transf\_auth”}(\text{id} = t_k)^D, a_k \notin R_b \wedge v_k + \sum_i (v_i \mid a_i \notin R_b) > 500 : (“registered”, R_b) \in P_{TA}(\text{ETF}, b)$
- 7)  $[(u, b) \text{“transf\_forms”}(\text{val} = v, \text{dest} = a)(\text{id} = t)^A \rightarrow (u, b) \text{“transf\_auth”}(\text{id} = t)^A]^I \rightarrow (u, b) \text{“transf\_forms”}(\text{val} = v_k, \text{dest} = a_k)(\text{id} = t_k)^A \Rightarrow (u, b) \text{“transf\_auth”}(\text{id} = t_k)^D, a_k \hat{\vdash} R_b \dot{\cup} v_k + \hat{\Delta} v_i > 1500 : (“registered”, R_b) \in P_{TA}(\text{ETF}, b)$

For properly analyzing the conceived scenario, besides these 7 rules, each restriction on workflow sequence must also generate an additional rule, stating, for instance, that the approval of an EFT (action “transf\_auth”) must always follow its definition (action “transf\_forms”).

### B. Writing State-Space Predicates

Given a set of initial conditions, namely the pre-programmed parameters of each user and account and the set of all (relevant) possible requests for the WFMS, the resulting CPN of the model can be analyzed to generate the graph of all possible states it may assume. Since the number of these states is most likely too large to allow a manual analysis, CPN Tools allows the modeler to automate the search for states with specific properties by executing queries that describe these properties and filter the state-space.

Every security rule described as above states a sufficient though not necessary condition for the outcome of the request to which it refers. Consequently, if a rule states that a request R is to be denied when it satisfies the conditions  $\alpha$ , to test that rule one must search for states where R satisfies the conditions  $\alpha$ , and yet it has been authorized. Since the state-space analysis is designed to cover all possible situations, if no such state can be found, then the rule has been followed.

In CPN Tools, the function `PredAllNodes` allows one to filter the generated state-space according to some predicate function, usually stating properties of a marking. Also, combining functions `InArcs` and `SourceNodes`, one may obtain a list of the immediate predecessor states to any desired state. Applying these recursively, it is possible to generate the ordered lists of all acyclical paths leading to the states that satisfy the right-hand side of any rule. With the help of functions `PredAllScCs` and `ScCToNodes`, it is also possible to determine all sets of states forming cycles in the state-space graph. Therefore, testing any rule expressed in our given notation becomes a matter of verifying the presence or

absence of states representing the rule’s restrictions within the lists for some or all paths leading to a set of states.

For most rules, however, some simplification is possible and desirable for optimizing performance. The following pseudocode shows the structure of the query for rule (7), which is a good example of a highly complex rule.

- 1: `auths`  $\leftarrow$  all states where a “transf\_auth” action has been authorized
- 2: **for all** states  $s_1$  in `auths` **do**
- 3:   **if**  $s_1$  is in a state-space cycle **then**
- 4:     add  $s_1$  to `insecure_states`
- 5:   **end if**
- 6:   **for all** states  $s_2$  in acyclical paths  $p$  from  $s_1$  back to 1 **do**
- 7:     **if** a “transf\_auth” action has been authorized in  $s_2$  **and** `account( $s_2$ ) = account( $s_1$ )` **and** `user( $s_2$ ) = user( $s_1$ )` **then**
- 8:       add parameter `tid` from  $s_2$  to list  $t$
- 9:     **end if**
- 10:    **if** a “transf\_forms” action has been authorized in  $s_2$  **and** `account( $s_2$ ) = account( $s_1$ )` **and** `user( $s_2$ ) = user( $s_1$ )` **and** parameter `acc` from  $s_2$  is in the registered accounts list from `account( $s_1$ )` **and** parameter `tid` from  $s_2$  is in list  $t$  **then**
- 11:      `limit_consumed`  $\leftarrow$  `limit_consumed` + (parameter `val` from  $s_2$ )
- 12:      remove `tid` from list  $t$
- 13:    **end if**
- 14:    **end for**
- 15:    `largest_limit_consumed` = `max(limit_consumed)` in  $p$
- 16:    **if** `largest_limit_consumed` > 1500 **then**
- 17:      add  $s_1$  to `insecure_states`
- 18:    **end if**
- 19: **end for**
- 20: **return** `insecure_states`

The syntax and auxiliary functions for navigating the state-space are all properly documented in [8].

With this logic for rule validation, there is no need for the modeler to tamper with the state definitions adding extra information to function as clues for identifying the trail of states while analyzing a single PN marking. Such a technique will always increase the total number of states in an analysis. Another avoided pitfall is the writing of predicates that reason about inner states of the model linked to decisions about modeling rather than system specification — doing so increases the risk of using false arguments to attest properties of the model.

### C. Preventing State-Space Explosion

In many workflow systems, as is the case in [6], [9] among others, the possible sequences of actions that can be requested by a user are few, and may be completely included in the model. However, there are systems where a wider variety of possibilities exist, causing any attempt to model all possible workflows to generate a state-space too large for analysis. For such cases, the analysis must be subdivided in a way that combining each division’s independent analysis yields the same conclusions as the analysis made as a whole.

It is reasonable to assume that, for most systems, different tasks often consist of independent workflows and, therefore, tasks or groups of tasks could be the pivotal elements of the necessary subdivision. Our metamodel, expecting such a need, effectively separates the data domains that constitute the inner state of each task. Let us recall that the decision regarding a request in a WFMS is a function of the parameters from a pair (account, task), whereas the update function for these parameters is executed for all tasks. In practice, this means that when updating a state, a request from a certain task may or may not alter the parameters for another task at will, but the decision is always based solely on parameters exclusive for the task that encompasses the processing request.

By cleverly comparing the parameters of a task in the states immediately preceding and immediately following the processing of a request, we may conclude whether that request causes a change in state in the scope of the task observed. If by doing so for both an authorization and a denial of the same action, we verify that the parameters remain unchanged, than that action is proven independent of the observed task, and may be excluded from the analysis of that particular task. Exceptions must be made for the cases when the action alters the session parameters, which are shared globally by all tasks, and, more subtly, when that action influences the outcome of a different action, which in turn affects the task under analysis.

As an additional simplification, unless the policy contains some rule such as rule (2) from the example, where consequences of a denied request are specified, the update functions for denied cases should not alter the state of the system and, therefore, the receiving of a denied response could be used as condition for terminating a workflow, preventing several cyclical paths from being calculated and speeding up the evaluation of predicates.

Preventing state-space explosion involves making intelligent assumptions or simplifications during the modeling [10] and the acceptable limits of state-space size and calculation time depend on the application. Merely as a reference, table II lists the number of states generated for various conditions in the example policy based on an initial set of 7 well-formed requests, one of each existing actions, requested by a “master” user in account 1.

The results shown indicate that the state-space is generally more sensitive to an increase in the number of different accounts than request variations on its workload. That fact may be understood as the effect of the several different intermediate states caused by the multiple possible orderings in which each request may be sent to the server when many clients are accessing it simultaneously. It is important to notice, though, that tolerating larger workflows for a single client is a very positive feature, since it allows the conception of test cases that test the dependency between sequences of operations in the model, which is the likely case where no subdivision in the suggested fashion is possible. Putting together that fact, the various possible mechanisms discussed for reducing state-space size, the treatability of the general structure of queries for rules, and the successful analysis of the example case, there is good evidence of the adequacy of the modeled policy for the intended analysis.

TABLE II. NUMBER OF STATE-SPACE NODES FOR DIFFERENT WORKLOAD CONDITIONS

Workload condition (in relation to base case)	Request variations	States
Base case	7	1122
Wrong login password	7	86
Wrong EFT password	7	470
“helper” user	7	470
EFT of \$500 instead of \$250	7	860
+ Request for “transf_auth” with other “tid”	8	1845
Two previous tests combined	8	1113
Misc. variations of parameters	14	58911
Base requests also for “helper” on same acc.	14	13997
Base requests also for “master” on other acc.	14	104320

## V. RELATED WORK

A significant difference between our approach and all others in the line of [6], is that their analyses [11], [12] are focused on finding a state with insecure properties whereas ours determines an insecure condition by locating an insecure state *path*. By adopting this concept, we introduce a trade-off between state-space graph search time and state-space size, which, to our knowledge, hasn’t been investigated in the literature for this area.

The definition of a *value dependency* given in [11] suits our ultimate CPN translation of a complex business rule, however, modeling as they propose requires knowledge of all possible outcomes of calculations at design time making the task impractical whereas, thanks to the concept of colored tokens, we are able to differentiate states assigning the result of a calculation to a token simplifying the design.

Other differences include our definition of a metamodel in a higher level of abstraction, which allowed us to adopt certain general assumptions in the analysis. As a side note, the example model from [12] of a document release process could be modeled using our strategy by representing the document resource as a property in an *editing* task within an account, and setting its value to represent the user currently allowed to perform actions in its workflow.

A different approach, adopted in SecureUML [13], aims at dealing with complex systems security by orienting their design and translating the resulting specification into a formal security policy model. Even though their metamodel is generally more comprehensive than ours, it is not targeted at dealing with workflows and complex business logic. Moreover, the analysis they propose [14] mentions that support for handling system state, which could include the analysis of workflows as we propose, would require reasoning about consequences of their specification’s formulas, and has been left for future work.

More recently, a process of analysis of RBAC models [15] in workflows using CPN has been described [16] that shares many characteristics with ours. Much like with the previous examples, this formalization also lacks the ability to express constraints related to the business parameters.

Finally, in [9], the authors define an approach to testing which closely resembles ours, in that the generation of mutants is equivalent to our enumeration of possible input requests. Besides the omission in treatment of business-related rules as in the previous models, the authors mention that for larger systems, analyzing reachability trees could require dividing the system into independent submodules but provide no insight into how such division could be handled. By introducing the notion of restrict data domains for state updates, we have taken a larger step in providing an orientation for the division of these larger systems.

## VI. CONCLUSIONS

The success in modeling the security policy from the example indicates that we have achieved a definition for the metamodel that satisfies the requirement of expressing complex authorization logic linked to parameters from the business model. The communication-based description of rules and its translation into predicates of the model's state-space provide a viable method of ensuring the model's proper behavior and guaranteeing consistency in a given set of rules. The state-space explosion problem was avoided by means of a combination of minimal metamodel design, state-space queries that include conditions on paths to states, and especially a roadmap for subdivision of analysis with guaranteed equivalence of results.

The method of analysis discussed is sufficient to attest whether a modeled security policy is consistent. However, demonstrating its completeness and non-redundancy requires not only the conclusion that the metamodel fully represents the policy's description as also that they are equivalent. A possibility within the existing framework is to analyze the metamodel state-space and derive a set of rules from the behavior it implies, later matching those rules to the original policy description. Since the proposed definition of metamodel also supports that method of analysis, we have achieved our goal of providing an approach to modeling security policies rich with business logic that is suitable for a complete analysis.

We believe that security policy models built with the formalization provided here result in specifications that represent systems behavior in a low level of abstraction, simplifying their implementation in actual code and bringing an extra value to its adoption.

## VII. FUTURE WORK

As outlined above, a method for ensuring completeness and non-redundancy of a policy specification is desired. The method should also include a formalization of the communication-based description language for aiding precise specifications.

Additionally, another dimension of data referring to *context* is desired in the metamodel for signaling overall states of the system, such as "Wednesday" or "raining", to be controlled by special system requests included in the workflow. Other changes allowing a more direct modeling of RBAC and role administration as well as simplifying safe subdivision of analysis are also intended.

## REFERENCES

- [1] C. Petri, "Kommunikation mit automaten," Ph.D. dissertation, Institut für instrumentelle Mathematik, Bonn, 1962.
- [2] W. Aalst, "Three good reasons for using a petri-net-based workflow management system," *Information and Process Integration in Enterprises*, pp. 161–182, 1998.
- [3] K. Jensen, "Coloured petri nets," *Petri nets: central models and their properties*, pp. 248–299, 1987.
- [4] A. Ratzer, L. Wells, H. Lassen, M. Laursen, J. Qvortrup, M. Stissing, M. Westergaard, S. Christensen, and K. Jensen, "Cpn tools for editing, simulating, and analysing coloured petri nets," *Applications and Theory of Petri Nets 2003*, pp. 450–462, 2003.
- [5] V. Atluri and W. Huang, "An extended petri net model for supporting workflows in a multilevel secure environment," in *Proc. of the IFIP Working Conference on Database Security*, 1996, pp. 199–216.
- [6] V. Atluri and W. Huang, "An authorization model for workflows," in *Computer Security — ESORICS 96*, ser. Lecture Notes in Computer Science, E. Bertino, H. Kurth, G. Martella, and E. Montolivo, Eds. Springer Berlin / Heidelberg, 1996, vol. 1146, pp. 44–64.
- [7] P. Chen, "The entity-relationship model – toward a unified view of data," *ACM Transactions on Database Systems (TODS)*, vol. 1, no. 1, pp. 9–36, 1976.
- [8] K. Jensen, S. Christensen, and L. Kristensen, "Cpn tools state space manual," *Department of Computer Science, University of Aarhus*, 2006.
- [9] D. Xu, L. Thomas, M. Kent, T. Mouelhi, and Y. Le Traon, "A model-based approach to automated testing of access control policies," in *Proceedings of the 17th ACM symposium on Access Control Models and Technologies*. ACM, 2012, pp. 209–218.
- [10] J. Groote, T. Kouters, and A. Osaiweran, "Specification guidelines to avoid the state space explosion problem," *Fundamentals of Software Engineering*, pp. 112–127, 2012.
- [11] N. Adam, V. Atluri, and W. Huang, "Modeling and analysis of workflows using petri nets," *Journal of Intelligent Information Systems*, vol. 10, no. 2, pp. 131–158, 1998.
- [12] V. Atluri and W.-K. Huang, "A petri net based safety analysis of workflow authorization models," *Journal of Computer Security*, vol. 8, no. 2/3, pp. 209–240, 2000.
- [13] D. Basin, J. Doser, and T. Lodderstedt, "Model driven security for process-oriented systems," in *Proceedings of the eighth ACM symposium on Access Control Models and Technologies*. ACM, 2003, pp. 100–109.
- [14] D. Basin, M. Clavel, J. Doser, and M. Egea, "Automated analysis of security-design models," *Information and Software Technology*, vol. 51, no. 5, pp. 815–831, 2009.
- [15] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38–47, 1996.
- [16] H. Rakkay and H. Boucheneb, "Security analysis of role based access control models using colored petri nets and cpntools," in *Transactions on Computational Science IV*, ser. Lecture Notes in Computer Science, M. Gavrilova, C. Tan, and E. Moreno, Eds. Springer Berlin / Heidelberg, 2009, vol. 5430, pp. 149–176.



# A New Approach to Decoding of Rational Irreducible Goppa code

Ahmed DRISSI

LabSiv : Laboratoire des Systèmes informatiques et Vision  
ESCAM : Equipe de la Sécurité, Cryptographie, Contrôle d'Accès et Modélisation  
Departments of Mathematics and Computer Science  
Faculty of Sciences, Ibn Zohr University, Agadir, Morocco

Ahmed ASIMI

LabSiv : Laboratoire des Systèmes informatiques et Vision  
ESCAM : Equipe de la Sécurité, Cryptographie, Contrôle d'Accès et Modélisation  
Departments of Mathematics and Computer Science  
Faculty of Sciences, Ibn Zohr University, Agadir, Morocco

**Abstract—** The interesting properties of classical Goppa code and its effective decoding algorithm (algorithm of patterson) make the most appropriate candidate for use in the MC Eliece cryptosystem. Information leakage which results from the relationship between the error vector weight and the number of iterations in the decoding algorithm, presented a weakness of the cryptosystem. In this paper, we introduce a new approach to decoding, the use of binary Goppa code in system design MC Eliece which solve the problem of the leak of information, on the contrary in case of patterson algorithm. We treat this decoding method using the Newton identities and results of linear algebra.

**Keywords:** Binary Goppa code, the Newton identities, circulant matrix

## I-INTRODUCTION

A motivation of this work is to find algorithms for decoding binary Goppa code where their use in the design of the MC Eliece leaves no information leakage. To attack the system Mc Eliece, the researchers H.Gregor Molter.Marc Stottinger.Abdulhadi Shoufan.Falko Strenzke have exploited in [1] an information leak, which results from the relationship between the weight error vector and the number of iterations of the Euclidean algorithm extended used in the algorithm of Patterson, and extract the error vector which is secret, and thereafter the plaintext. it prompts us to seek another decoding algorithm where this leak information about the error is remedied. Magali Bardet used in [2] and [3] the Newton identities for decoding cyclic codes but also used the Grobner basis calculation and the theory of elimination. The similarity in structure between the control matrix of a cyclic code and a Goppa code has encouraged us to try to follow the same path, but it has happened

that the use of the properties of circular matrices and diagonalization better for our code.

In the next section, we state the notations used in this document and the third we define the Goppa code binary, its characterization and its correction capability. For the fourth section, it was replaced problem of solving a system in  $F_{2^m}^n$  to  $m$  systems in  $F_2^n$ . and its resolutions are discussed in the following two sections treating the relationship between Newton and elementary symmetric functions. Transforming this relationship in matrix form and use the properties of linear algebra, in particular the structure of a circulant matrix. We finally give our own method for decoding a binary irreducible Goppa code.

## II- NOTATIONS AND PRELIMINARIES

$m$  : An integer.

$F_{2^m}$  : A finite field of  $2^m$  elements.

$F_2 = \{0,1\}$ .

$F_2^n$  : The set of vectors of length  $n$  of a component 0 or 1.

$F_{2^m}^n$  : The set of vectors of length  $n$  a component of  $F_{2^m}$ .

$I_n$  : The identity matrix of size  $n$ .

$I$  : an identity matrix.

$I_d$  : The application identity.

$mat_\beta(f)$  : The matrix associated with the endomorphism  $f$  in the base  $\beta$ .

$\frac{d\sigma_a(x)}{dx}$  : The derivative of the polynomial  $\sigma_a(x)$  relative to  $x$ .

$\Gamma(L, g)$  : The Goppa code of support  $L$  and polynomial  $g$ .

$\lfloor \rfloor$  : The integer part.

$(w_1, \dots, w_m)$  : the basis of the vector space  $F_{2^m}$  on the field  $F_2$ .

$F_{2^m}[x]$  : The set of polynomials with coefficients in  $F_{2^m}$ .

$N$  : The set of integers.

$card$  : the number of elements of a set.

$rg(C)$  : the rank of a matrix  $C$

Let  $\alpha \in F_{2^m}$  and

$g(x) = g_0 + g_1x + \dots + g_rx^r \in F_{2^m}[x]$  with

$g_r \neq 0$ ;

$$g(x) - g(\alpha) = g_1(x - \alpha) + \dots + g_r(x^r - \alpha^r) = (x - \alpha) \sum_{k=1}^r g_k \sum_{j=0}^{k-1} x^j \alpha^{k-1-j}$$

Therefore

$$\frac{-g(x)}{g(\alpha)} + 1 = (x - \alpha) \left[ -\frac{1}{g(\alpha)} \sum_{k=1}^r g_k \left( \sum_{i=0}^{k-1} x^i \alpha^{k-1-i} \right) \right];$$

It is said that

$$\frac{1}{x - \alpha} \bmod g(x) = -\frac{1}{g(\alpha)} \sum_{k=1}^r g_k \left( \sum_{i=0}^{k-1} x^i \alpha^{k-1-i} \right).$$

### III- The Binary Goppa code

#### 1-Definition

Let  $L = (\alpha_1, \dots, \alpha_n)$  a sequence of  $n$  distinct elements of  $F_{2^m}$  and  $g(x) \in F_{2^m}[x]$  a polynomial of degree  $r$  in  $F_{2^m}[x]$  such as  $1 \leq r \leq n-1$  and  $g(\alpha_i) \neq 0$  for all  $i = 1, \dots, n$ .

Rational Goppa code of support  $L$  (vector generator) and of generator polynomial  $g$  (Goppa polynomial) noted  $\Gamma(L, g)$  is the set

$$\Gamma(L, g) = \left\{ c = (c_1, \dots, c_n) \in F_2^n / \sum_{i=1}^n c_i \left( \frac{1}{x - \alpha_i} \bmod g(x) \right) = 0 \right\}$$

If  $g$  is irreducible, we say that  $\Gamma(L, g)$  is an irreducible binary Goppa code.

#### 2- Characterization of Goppa code

##### Theorem

Let  $L = (\alpha_1, \dots, \alpha_n)$  a sequence of  $n$  distinct elements of  $F_{2^m}$  and  $g(x) \in F_{2^m}[x]$  a

polynomial of degree  $r$  in  $F_{2^m}[x]$ , such as  $1 \leq r \leq n-1$  and  $g(\alpha_i) \neq 0$  for all  $i = 1, \dots, n$ .

It has the three following assertions are equivalent:

$$i) \sum_{i=1}^n a_i \left( \frac{1}{x - \alpha_i} \bmod g(x) \right) = 0.$$

$$ii) Ha^t = 0 \text{ with}$$

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \dots & \dots & \dots & \dots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \dots & \alpha_n^{r-1} \end{pmatrix} \begin{pmatrix} g(\alpha_1)^{-1} \\ \dots \\ g(\alpha_n)^{-1} \end{pmatrix}$$

$H$  is called control matrix Goppa code  $\Gamma(L, g)$

$$iii) g(x) \text{ divided } \frac{d\sigma_a(x)}{dx} \text{ with}$$

$$\sigma_a(x) = \prod_{i=1}^n (x - \alpha_i)^{a_i}.$$

##### proof

we have

$$\begin{aligned} \frac{1}{x - \alpha} \bmod g(x) &= -\frac{1}{g(\alpha)} \sum_{k=1}^r g_k \left( \sum_{i=0}^{k-1} x^i \alpha^{k-1-i} \right); \\ \sum_{i=1}^n a_i \frac{1}{x - \alpha_i} \bmod g(x) &= -\sum_{i=1}^n a_i g(\alpha_i)^{-1} \left( \sum_{k=1}^r g_k \sum_{j=0}^{k-1} x^{k-1-j} \alpha_i^j \right) \\ &= -\sum_{k=1}^r g_k \sum_{j=0}^{k-1} x^{k-1-j} \left( \sum_{i=1}^n a_i g(\alpha_i)^{-1} \alpha_i^j \right) \\ &= -\sum_{k=1}^r g_k \sum_{j=0}^{k-1} x^{k-1-j} A_j \end{aligned}$$

we denote

$$A_j = \sum_{i=1}^n a_i g(\alpha_i)^{-1} \alpha_i^j, j = 0, 1, \dots, r-1.$$

$$ii) \Rightarrow i)$$

$$Ha^t = 0 \Rightarrow \sum_{i=1}^n a_i g(\alpha_i)^{-1} \alpha_i^j = 0 \text{ pour } j = 0, 1, \dots, r-1 \text{ then}$$

$$\sum_{i=1}^n a_i \frac{1}{x - \alpha_i} \bmod g(x) = 0.$$

$$i) \Rightarrow ii)$$

$$\text{Let } \sum_{i=1}^n a_i \frac{1}{x - \alpha_i} \bmod g(x) = 0, \text{ therefore}$$

$$\sum_{k=1}^r g_k \sum_{j=0}^{k-1} x^{k-1-j} A_j = 0 \text{ then}$$

$$\begin{aligned} &g_1 A_0 + g_2 (x A_0 + A_1) + g_3 (x^2 A_0 + x A_1 + A_2) + \\ &g_4 (x^3 A_0 + x^2 A_1 + x A_2 + A_3) + g_5 (x^4 A_0 + x^3 A_1 + \\ &+ x^2 A_2 + x A_3 + A_4) + \dots \\ &+ g_r (x^{r-1} A_0 + x^{r-2} A_1 + \dots + x A_{r-2} + A_{r-1}) = 0 \end{aligned}$$

Then

$$\begin{aligned} g_1 A_0 + g_2 A_1 + g_3 A_2 + \dots + g_r A_{r-1} &= 0 \\ g_2 A_0 + g_3 A_1 + \dots + g_r A_{r-2} &= 0 \\ g_3 A_0 + \dots + g_r A_{r-3} &= 0 \\ \dots \\ g_{r-2} A_0 + g_r A_1 &= 0 \\ g_r A_0 &= 0. \end{aligned}$$

Since  $g_r \neq 0$ , it was  $A_0 = 0$ .

By recurrence we find that  $A_j = 0$  for

$$j = 0, 1, \dots, r-1.$$

i)  $\Leftrightarrow$  iii)

$$\begin{aligned} \frac{d\sigma_a(x)}{dx} &= \sum_{i=1}^n a_i (x - \alpha_i)^{a_i-1} \prod_{\substack{j=1 \\ j \neq i}}^n (x - \alpha_j)^{a_j} = \sum_{i=1}^n \frac{a_i}{x - \alpha_i} \prod_{j=1}^n (x - \alpha_j)^{a_j} \\ &= \sigma_a(x) \cdot \sum_{i=1}^n \frac{a_i}{x - \alpha_i} = \sigma_a(x) \cdot R_a(x). \end{aligned}$$

$$\text{It was } R_a(x) = \sum_{i=1}^n \frac{a_i}{x - \alpha_i} = \frac{P(x)}{Q(x)} \text{ with}$$

$$Q(x) = \prod_{i=1}^n (x - \alpha_i) \text{ and}$$

$$u_i(x) = \frac{1}{x - \alpha_i} \bmod g(x).$$

It was  $u_i(x) \cdot (x - \alpha_i) = 1 + k_i(x) \cdot g(x)$

$$\begin{aligned} \sum_{i=1}^n a_i \left( \frac{1}{x - \alpha_i} \bmod g(x) \right) &= \sum_{i=1}^n a_i u_i(x) \\ &= \sum_{i=1}^n \frac{a_i}{x - \alpha_i} + \sum_{i=1}^n \frac{a_i k_i(x) g(x)}{x - \alpha_i} \\ &= R_a(x) + g(x) \sum_{i=1}^n a_i \frac{k_i(x)}{x - \alpha_i} \\ &= \frac{P(x)}{Q(x)} + g(x) \sum_{i=1}^n a_i \frac{k_i(x)}{x - \alpha_i} \end{aligned}$$

Where

$$Q(x) \cdot \sum_{i=1}^n a_i \left( \frac{1}{x - \alpha_i} \bmod g(x) \right) = P(x) + g(x) \cdot Q(x) \cdot \sum_{i=1}^n a_i \frac{k_i(x)}{x - \alpha_i} \quad (1)$$

$$\text{If } \sum_{i=1}^n a_i \left( \frac{1}{x - \alpha_i} \bmod g(x) \right) = 0 \text{ then } g(x)$$

divided  $P(x)$  (indeed  $Q(x) \cdot \sum_{i=1}^n a_i \frac{k_i(x)}{x - \alpha_i}$  is a

polynomial) gold it was  $\frac{d\sigma_a(x)}{dx} = \sigma_a(x) \cdot R_a(x)$

then  $Q(x) \cdot \frac{d\sigma_a(x)}{dx} = \sigma_a(x) \cdot P(x)$  therefore

$g(x)$  divided  $Q(x) \cdot \frac{d\sigma_a(x)}{dx}$ ; gold  $Q(x)$  and

$g(x)$  are mutually prime (because  $g(\alpha_i) \neq 0, i = 1, \dots, n$ ) therefore  $g(x)$  divided

$$\frac{d\sigma_a(x)}{dx} \Leftrightarrow$$

If  $g(x)$  divided  $\frac{d\sigma_a(x)}{dx}$  therefore  $g(x)$

divided  $Q(x) \cdot \frac{d\sigma_a(x)}{dx} = \sigma_a(x) \cdot P(x)$  and since

$g(x)$  and  $\sigma_a(x)$  are mutually prime therefore  $g(x)$  divided  $P(x)$  and according to (1)  $g(x)$

divided  $Q(x) \cdot \sum_{i=1}^n a_i \left( \frac{1}{x - \alpha_i} \bmod g(x) \right)$  and

since  $g(x)$  and  $Q(x)$  are mutually prime then

$g(x)$  divided  $\sum_{i=1}^n a_i \left( \frac{1}{x - \alpha_i} \bmod g(x) \right)$ . We

know that  $\deg g(x) = r$  and

$\deg \left( \sum_{i=1}^n a_i \left( \frac{1}{x - \alpha_i} \bmod g(x) \right) \right) = r-1$  then

$$\sum_{i=1}^n a_i \left( \frac{1}{x - \alpha_i} \bmod g(x) \right) = 0$$

### 3- correction capacity

The parity matrix  $H$  can be written as the product of a Vandermonde matrix and a nonsingular matrix so any square submatrix  $r \times r$  of  $H$  is invertible, then there is no code word of weight less or equal to  $r$ , then it has a minimum

distance of at least  $d = r + 1$  (of capacity correction  $[\frac{r}{2}]$ ).

If we add an additional constraint on  $g$  to be without multiple factors, we can double the capacity of correction. (in particular irreducible codes).

Indeed  $g(x)$  divided  $\frac{d\sigma_a(x)}{dx}$ , gold on  $F_{2^m}$  the derivative of a polynomial does not contain coefficients of odd degree, therefore there exists a polynomial satisfying  $\frac{d\sigma_a(x)}{dx} = f^2(x)$ .

If  $g$  has no multiple factors and  $g$  divided  $f^2$  then,  $g$  necessarily divided  $f$ .

A word  $a$  which belongs to the code  $\Gamma(L, g)$  with  $g$  without multiple factors belong to the code  $\Gamma(L, g^2)$  which has a minimum distance  $2r + 1$  and a decoding algorithm to  $r$  errors.

### 4- The decoding

Formally the decoding problem can be stated as follows: let the received word  $r = (r_1, r_2, \dots, r_n)$  and the codeword sent  $c = (c_1, c_2, \dots, c_n)$  such as  $r = c + e$  with  $e = (e_1, e_2, \dots, e_n)$  a weight vector less or equal to the correction capacity

$$\begin{pmatrix} S_0 \\ S_1 \\ \dots \\ S_{r-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \dots & \dots & \dots & \dots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \dots & \alpha_n^{r-1} \end{pmatrix} \begin{pmatrix} g(\alpha_1)^{-1} \\ \dots \\ g(\alpha_n)^{-1} \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ \dots \\ r_n \end{pmatrix} \\ = Hr^t = Hc^t + He^t = 0 + He^t = He^t \\ = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \dots & \dots & \dots & \dots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \dots & \alpha_n^{r-1} \end{pmatrix} \begin{pmatrix} g(\alpha_1)^{-1} \\ \dots \\ g(\alpha_n)^{-1} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ \dots \\ e_n \end{pmatrix} \\ = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \dots & \dots & \dots & \dots \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \dots & \alpha_n^{r-1} \end{pmatrix} \begin{pmatrix} g(\alpha_1)^{-1}e_1 \\ g(\alpha_2)^{-1}e_2 \\ \dots \\ g(\alpha_n)^{-1}e_n \end{pmatrix}$$

$$\begin{pmatrix} g(\alpha_1)^{-1}e_1 \\ g(\alpha_2)^{-1}e_2 \\ \dots \\ g(\alpha_n)^{-1}e_n \end{pmatrix}$$

We must find the vector

$$\begin{pmatrix} S_0 \\ S_1 \\ \dots \\ S_{r-1} \end{pmatrix} \text{ is called the syndrome vector.}$$

we introduce the sequence of syndromes extended  $(S_i)_{i \in N}$

We see that  $S_{i+2^m-1} = S_i \forall i \in N$  therefore we restrict to the

finite sequence  $S_j = \sum_{i=1}^n \frac{e_i}{g(\alpha_i)} \alpha_i^j$  for  $j = 0, 1, \dots, 2^m - 2$ .

### IV -The Newton identities

Let  $k \in N$  and  $x_1, x_2, \dots, x_k \in F_{2^m}$ , the following theorem known as Newton's identity gives a relation between the elementary symmetric functions  $\sigma_j = \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq k} x_{i_1} \dots x_{i_j}$  and

the sums of newton  $S_p = \sum_{i=0}^k x_i^p, \forall p \in N$ .

#### Theorem -circular identity of Newton-

Let  $k \in N$ ,  $x_1, x_2, \dots, x_k \in F_{2^m}$ , the sums of newton

$S_i = \sum_{j=0}^k x_j^i, \forall i \in N$ , the elementary symmetric functions

$\sigma_1, \dots, \sigma_k$  of  $x_1, x_2, \dots, x_k$  defined by  $\sigma_j = \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq k} x_{i_1} \dots x_{i_j}$

then we will have relations  $S_i + \sum_{j=1}^k \sigma_j S_{i-j} = 0$  for  $i \geq k$ .

#### Proof

We denote the polynomial

$$\sigma(x) = \prod_{j=1}^k (x - x_j) = \sum_{j=0}^k \sigma_j x^{k-j} = \sigma_0 + \sigma_1 x^{k-1} + \dots + \sigma_{k-1} x + \sigma_k$$

with  $\sigma_0 = 1$ . For  $j$  fixed  $\sigma(x_j) = 0$  therefore  $\sigma_0 x_j^k + \sigma_1 x_j^{k-1} + \dots + \sigma_{k-1} x_j + \sigma_k = 0$

Let for  $p \geq k$   $x_j^{p-k} \sigma(x_j) = 0$  then

$$\sigma_0 x_j^p + \sigma_1 x_j^{p-1} + \dots + \sigma_{k-1} x_j^{p-k+1} + \sigma_k x_j^{p-k} = 0$$

Summing over  $j$  we will

$$\sigma_0 S_p + \sigma_1 S_{p-1} + \dots + \sigma_{k-1} S_{p-k+1} + \sigma_k S_{p-k} = 0$$

$$\text{Since } S_{i+2^m-1} = S_i \quad (\text{indeed } S_{i+2^m-1} = \sum_{j=1}^k x_j^{i+2^m-1} = \sum_{j=1}^k x_j^i = S_i)$$

therefore for

$$1 \leq p \leq k \quad \text{we will } S_{p+2^m-1} = S_p \quad \text{and } p+2^m-1 \geq k$$

then we can write this relation in matrix form as follows

**Lemma: form matrix identity newton**

Let  $x_1, x_2, \dots, x_k \in F_{2^m}$  and

$$\sigma(x) = \prod_{j=1}^k (x - x_j) = \sum_{j=0}^k \sigma_j x^{k-j} = \sigma_0 + \sigma_1 x^{k-1} + \dots + \sigma_{k-1} x + \sigma_k$$

and

$$S_i = \sum_{j=0}^k x_j^i, \quad \forall i = 0, 1, \dots, 2^m - 2 \quad \text{it was}$$

$$\begin{bmatrix} S_{2^m-2} & S_{2^m-3} & \dots & S_0 \\ S_0 & S_{2^m-2} & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2^m-3} & S_{2^m-4} & \dots & S_{2^m-2} \end{bmatrix} \begin{bmatrix} 0 \\ \dots \\ 0 \\ 1 \\ \sigma_1 \\ \dots \\ \sigma_k \end{bmatrix} = 0.$$

## V- The circulant matrix

### Definitions

A circulant matrix with coefficients in a finite  $F_{2^m}$  of size  $n$

$$\text{is a matrix of the form } C = \begin{bmatrix} c_0 & c_1 & \dots & c_{n-1} \\ c_{n-1} & c_0 & \dots & c_{n-2} \\ \dots & \dots & \dots & \dots \\ c_1 & c_2 & \dots & c_0 \end{bmatrix} \text{ with}$$

$$c_i \in F_{2^m} \quad \forall i \in \{0, 1, \dots, n-1\}$$

$$\text{The matrix } A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 1 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{bmatrix} \text{ is said to be elementary}$$

circulant matrix.

### Lemma1

Let  $A$  the circulant matrix elementary of size  $n$  and  $E_j$  a  $j^{\text{eme}}$  line of the identity matrix  $I_n$  it was

$$i) A^n = I_n$$

$$ii) E_j A^k = E_{(j+k) \bmod n} \quad \forall k = 1, \dots, n$$

### Proof

i) let  $\beta(e_1, e_2, \dots, e_n)$  a base and  $f$  the endomorphism such as  $A = \text{mat}_{\beta}(f)$ , we see that  $f(e_1) = e_n$  and  $\forall k = 2, \dots, n$ ,  $f(e_k) = e_{k+1}$ , we deduce easily that  $f^n = I_d$  that is to say  $A^n = I_n$ .

ii) by recurrence on  $k$  it was for  $k = 1$ ,  $E_j A = E_{j+1}$ .

Suppose that  $E_j A^k = E_{(j+k) \bmod n}$  then

$$E_j A^{k+1} = E_j A^k A = E_{(j+k) \bmod n} A = E_{(j+k+1) \bmod n}$$

### Lemma2

We can decompose the circulant matrix  $C$  defined above in the following manner  $C = c_0 I + c_1 A + \dots + c_{n-1} A^{n-1}$

### Proof

Using the fact that  $E_j A^k = E_{(j+k) \bmod n}$  it was

$$E_j (c_0 I + c_1 A + \dots + c_{n-1} A^{n-1}) = c_0 E_j + c_1 E_{j+1} + \dots + c_{n-1} E_{j+n-1} = E_j C$$

Therefore a  $j^{\text{eme}}$  line of  $C$  and of

$$c_0 I + c_1 A + \dots + c_{n-1} A^{n-1} \text{ are equal.}$$

### Lemma3

Let  $\alpha$  the primitive element of the finite field  $F_{2^m}$  therefore

$$\alpha^{2^m-1} = 1 \quad \text{and} \quad \text{the matrix}$$

$$P = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{2^m-2} \\ \dots & \dots & \dots & \dots \\ 1 & \alpha^{2^m-2} & \dots & \alpha^{(2^m-2)(2^m-2)} \end{bmatrix} = (\alpha^{ij})_{\substack{i=0,1,\dots,2^m-2 \\ j=0,1,\dots,2^m-2}} \text{ is}$$

invertible and its inverse is

$$P^{-1} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha^{2^m-2} & \dots & \alpha \\ \dots & \dots & \dots & \dots \\ 1 & \alpha^{(2^m-2)(2^m-2)} & \dots & \alpha^{(2^m-2)} \end{bmatrix} = (\alpha^{-ij})_{\substack{i=0,1,\dots,2^m-2 \\ j=0,1,\dots,2^m-2}}$$

### Proof

$$\text{Let } a_{il} = \sum_{j=0}^{2^m-2} \alpha^{ij} \alpha^{-jl} = \sum_{j=0}^{2^m-2} \alpha^{j(i-l)} = \begin{cases} 1 & \text{si } i = l \\ 0 & \text{si } i \neq l \end{cases}$$

$$\text{gold it was } 1 + \alpha + \alpha^2 + \dots + \alpha^{2^m-2} = 0 \text{ indeed } (1 - \alpha)(1 + \alpha + \alpha^2 + \dots + \alpha^{2^m-2}) = 1 - \alpha^{2^m-1} = 1 - 1 = 0$$

### Lemma 4

Let  $(c_1, c_2, \dots, c_{n-1}) \in F_{2^m}^n$  and the polynomial

$C(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$  it was if  $n = 2^m - 1$  and  $\alpha$  primitive root of the finite field  $F_{2^m}$

$$\begin{bmatrix} c_0 & c_1 & \dots & c_{n-1} \\ c_{n-1} & c_0 & \dots & c_{n-2} \\ \dots & \dots & \dots & \dots \\ c_1 & c_2 & \dots & c_0 \end{bmatrix} \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{n-2} \\ \dots & \dots & \dots & \dots \\ 1 & \alpha^{n-2} & \dots & \alpha^{(n-2)(n-3)} \end{bmatrix} \begin{bmatrix} C(1) \\ C(\alpha) \\ \dots \\ C(\alpha^{n-2}) \end{bmatrix} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha^{n-2} & \dots & \alpha \\ \dots & \dots & \dots & \dots \\ 1 & \alpha^{(n-2)(n-3)} & \dots & \alpha^{n-2} \end{bmatrix} \begin{bmatrix} C(\alpha^{n-2}) \\ C(\alpha^{n-3}) \\ \dots \\ C(\alpha) \end{bmatrix}$$

And  $rg(C) = card\{i \in \{0, 1, \dots, n-1\}, C(\alpha^i) \neq 0\}$

### Proof

Calculate the eigenvalues of the circulant matrix elementary  $A$  of size  $n$ .

It was  $A^{2^m-1} = I$  by Lemma 1.

Let  $\alpha$  primitive root of the finite field  $F_{2^m}$  (that is to say  $\alpha^{2^m-1} = 1$ ) it was

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & \alpha^i \\ & & & \dots & 0 \\ 0 & & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & \alpha^{i(2^m-2)} \end{bmatrix} \begin{bmatrix} 1 \\ \alpha^i \\ \dots \\ \alpha^{i(2^m-2)} \end{bmatrix} = \alpha^i \begin{bmatrix} 1 \\ \alpha^i \\ \dots \\ \alpha^{i(2^m-2)} \end{bmatrix} \text{ for } i = 0, 1, \dots, 2^m - 2$$

so we can diagonalize  $A$  as follows

$$A = P \begin{bmatrix} 1 & & & \\ & \alpha & & \\ & & \dots & \\ & & & \alpha^{2^m-2} \end{bmatrix} P^{-1} \text{ with } P = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{2^m-2} \\ \dots & \dots & \dots & \dots \\ 1 & \alpha^{2^m-2} & \dots & \alpha^{(2^m-2)(2^m-2)} \end{bmatrix}; \text{ gold it was } C = C(A) \text{ by lemma 2}$$

$$C = C(A) = C \left( P \begin{bmatrix} 1 & & & \\ & \alpha & & \\ & & \dots & \\ & & & \alpha^{2^m-2} \end{bmatrix} P^{-1} \right) = P \begin{bmatrix} C(1) & & & \\ & C(\alpha) & & \\ & & \dots & \\ & & & C(\alpha^{2^m-2}) \end{bmatrix} P^{-1}$$

and we deduce that also

$$rgC = rg \begin{bmatrix} C(1) & & & \\ & C(\alpha) & & \\ & & \dots & \\ & & & C(\alpha^{2^m-2}) \end{bmatrix} = card\{i \in \{0, 1, \dots, n-1\}, C(\alpha^i) \neq 0\}$$

### VI- FOR $F_{2^m}$ TO $F_2^m$

we put  $v = [v_1, \dots, v_n] \in F_{2^m}^n$  and we must solve the following system in  $F_{2^m}^n : Av^t = S$  with the matrix  $A$  and the vector  $S$  are known.

In this section we will replace this system by  $m$  systems unknown in  $F_2^n$

$$Av^\lambda = S^\lambda, \lambda = 1, \dots, m$$

Let  $(\omega_1, \dots, \omega_m)$  a base of  $F_{2^m}$  as a vector space on field  $F_2$

$$\forall v \in F_{2^m}; v = \sum_{\lambda=1}^m v_\lambda \omega_\lambda \text{ and } \forall s \in F_{2^m}; s = \sum_{\lambda=1}^m s_\lambda \omega_\lambda$$

Let  $A = (a_{ij})_{i=1 \dots r, j=1 \dots r}$  a matrix of elements in  $F_{2^m}$

Let the system  $Av^t = s$

For  $i = 1 \dots r$  it was

$$s_i = \sum_{j=1}^n a_{ij} v_j = \sum_{j=1}^n a_{ij} \left( \sum_{\lambda=1}^m v_j^\lambda \omega_\lambda \right) = \sum_{\lambda=1}^m \left( \sum_{j=1}^n a_{ij} v_j^\lambda \right) \omega_\lambda = \sum_{\lambda=1}^m s_i^\lambda \omega_\lambda$$

therefore  $s_i^\lambda = \sum_{j=1}^n a_{ij} v_j^\lambda$  we conclude that

$$\forall i = 1, \dots, n, v_i \in F_{2^m} \text{ we put } v_i = \sum_{\lambda=1}^m v_i^\lambda \omega_\lambda$$

$$\forall j = 1, \dots, 2r-1, s_j = \sum_{\lambda=1}^m s_j^\lambda \omega_\lambda \text{ therefore}$$

$$A \begin{bmatrix} v_1^1 & \dots & v_1^m \\ \vdots & \dots & \vdots \\ v_n^1 & \dots & v_n^m \end{bmatrix} = \begin{bmatrix} s_0^1 & \dots & s_0^m \\ \vdots & \dots & \vdots \\ s_{r-1}^1 & \dots & s_{r-1}^m \end{bmatrix}$$

### VII- SOLVING SYSTEMS OF VANDERMONDE MATRIX $F_2^n$

$$\text{Let the system } A \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} S_0 \\ \vdots \\ S_{2^m-2} \end{bmatrix}; \text{ if } A \text{ is of the form}$$

$$A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{2^m-2} & \alpha_2^{2^m-2} & \dots & \alpha_n^{2^m-2} \end{pmatrix}$$

$$\text{Suppose that the indices } i_1, \dots, i_k \text{ of vector } \begin{bmatrix} v_1 \\ \vdots \\ \vdots \\ v_n \end{bmatrix} \text{ are not zero}$$

that is to say  $v_{i_1} = \dots = v_{i_k} = 1$ ; it follows

$$S_0 = 1 + \dots + 1$$

$$S_1 = \alpha_{i_1} + \dots + \alpha_{i_k}$$

$$S_2 = \alpha_{i_1}^2 + \dots + \alpha_{i_k}^2$$

...

$$S_{2^m-2} = \alpha_{i_1}^{2^m-2} + \dots + \alpha_{i_k}^{2^m-2}$$

We put  $\alpha_{i_1} = x_1, \dots, \alpha_{i_k} = x_k$  therefore

$$S_i = \sum_{j=1}^k x_j^i, i = 0, 1, \dots, 2^m - 2$$

$$\text{Let } \sigma(x) = \prod_{j=1}^k (x - x_j) = \sum_{j=0}^k \sigma_j x^{k-j}$$

$$v_i = 1 \Leftrightarrow \sigma(\alpha_i) = 0$$

Just find the polynomial  $\sigma(x)$  and exhaustive search method known as one dog finds its roots and can be detected by following the indices  $i_1, \dots, i_k$ .

According to Newton's identity it was

$$\begin{bmatrix} S_{2^m-2} & S_{2^m-3} & \dots & S_0 \\ S_0 & S_{2^m-2} & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2^m-3} & S_{2^m-4} & \dots & S_{2^m-2} \end{bmatrix} \begin{bmatrix} 0 \\ \dots \\ 0 \\ 1 \\ \sigma_1 \\ \dots \\ \sigma_k \end{bmatrix} = 0; \text{ so we have to solve this}$$

system, first study the uniqueness of solution.

**Lemma**

$$\text{rg} \begin{bmatrix} S_{2^m-2} & S_{2^m-3} & \dots & S_0 \\ S_0 & S_{2^m-2} & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2^m-3} & S_{2^m-4} & \dots & S_{2^m-2} \end{bmatrix} = k$$

**Proof**

$$S_i = \sum_{j=1}^k x_j^i = \sum_{j=1}^n v_j \alpha_j^i, \forall i \in N$$

$$\begin{bmatrix} S_i \\ S_{i+1} \\ \dots \\ S_{i+2^m-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{2^m-1} & \alpha_2^{2^m-1} & \dots & \alpha_n^{2^m-1} \end{bmatrix} \begin{bmatrix} v_1 \alpha_1^i \\ v_2 \alpha_2^i \\ \dots \\ v_n \alpha_n^i \end{bmatrix}$$

$$C_s = \begin{bmatrix} S_{2^m-2} & S_{2^m-3} & \dots & S_0 \\ S_0 & S_{2^m-2} & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2^m-3} & S_{2^m-4} & \dots & S_{2^m-2} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{2^m-1} & \alpha_2^{2^m-1} & \dots & \alpha_n^{2^m-1} \end{bmatrix} \begin{bmatrix} v_1 \alpha_1^{2^m-1} & \dots & v_1 \alpha_1 & v_1 \\ v_2 \alpha_2^{2^m-1} & \dots & v_2 \alpha_2 & v_2 \\ \dots & \dots & \dots & \dots \\ v_n \alpha_n^{2^m-1} & \dots & v_n \alpha_n & v_n \end{bmatrix}$$

$$= F \begin{bmatrix} v_1 & 0 & \dots & 0 \\ 0 & v_2 & \dots & \dots \\ \dots & \dots & \dots & 0 \\ 0 & \dots & \dots & v_n \end{bmatrix} F' \text{ with } F \text{ and } F' \text{ two matrices}$$

Vandermonde invertible therefore

$$\text{rg}(C_s) = \text{card}\{j \in \{1, \dots, n\} / v_j = 1\} = k$$

**Lemma**

We put for  $i = 0, 1, \dots, 2^m - 2$ ,  $S_i = \sum_{j=1}^n v_j \alpha_j^i$  and

$$\sigma(x) = \sum_{j=0}^k \sigma_j x^{k-j}$$

$$\text{The solution } \begin{bmatrix} 0 \\ \dots \\ 0 \\ 1 \\ \sigma_1 \\ \dots \\ \sigma_k \end{bmatrix} \text{ of system}$$

$$\begin{bmatrix} S_{2^m-2} & S_{2^m-3} & \dots & S_0 \\ S_0 & S_{2^m-2} & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2^m-3} & S_{2^m-4} & \dots & S_{2^m-2} \end{bmatrix} \begin{bmatrix} 0 \\ \dots \\ 0 \\ 1 \\ \sigma_1 \\ \dots \\ \sigma_k \end{bmatrix} = 0 \text{ of unknown } \begin{bmatrix} 0 \\ \dots \\ 0 \\ 1 \\ \sigma_1 \\ \dots \\ \sigma_k \end{bmatrix} \text{ is}$$

unique.

**Proof**

Repeat the same proof as above we obtain the lemma

$$\begin{bmatrix} S_k & S_{k-1} & \dots & S_0 \\ S_{k+1} & S_k & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2k-1} & S_{2k-2} & \dots & S_{k-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_n^{k-1} \end{bmatrix} \begin{bmatrix} v_1 & 0 & \dots & 0 \\ 0 & v_2 & \dots & \dots \\ \dots & \dots & \dots & 0 \\ 0 & \dots & \dots & v_n \end{bmatrix} \begin{bmatrix} \alpha_1^{k-1} & \dots & \alpha_1 & 1 \\ \alpha_2^{k-1} & \dots & \alpha_2 & 1 \\ \dots & \dots & \dots & \dots \\ \alpha_n^{k-1} & \dots & \alpha_n & 1 \end{bmatrix}$$

$$\text{So } \text{rg} \begin{bmatrix} S_k & S_{k-1} & \dots & S_0 \\ S_{k+1} & S_k & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2k-1} & S_{2k-2} & \dots & S_{k-1} \end{bmatrix} = k \text{ then}$$

$$\begin{bmatrix} S_k & S_{k-1} & \dots & S_0 \\ S_{k+1} & S_k & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2k-1} & S_{2k-2} & \dots & S_{k-1} \end{bmatrix}$$

is invertible.

$$C_s^{-1} \begin{bmatrix} 0 \\ \dots \\ 0 \\ 1 \\ \sigma_1 \\ \dots \\ \sigma_k \end{bmatrix} = 0 \Rightarrow \begin{bmatrix} S_k & S_{k-1} & \dots & S_0 \\ S_{k+1} & S_k & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2k-1} & S_{2k-2} & \dots & S_{k-1} \end{bmatrix} \begin{bmatrix} 1 \\ \sigma_1 \\ \dots \\ \sigma_k \end{bmatrix} = 0 \Rightarrow \begin{bmatrix} S_{k-1} & S_{k-2} & \dots & S_0 \\ S_k & S_{k-1} & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2k-2} & S_{2k-3} & \dots & S_{k-1} \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \dots \\ \sigma_k \end{bmatrix} = \begin{bmatrix} S_k \\ S_{k+1} \\ \dots \\ S_{2k-1} \end{bmatrix}$$



Since  $\begin{bmatrix} S_{k-1} & S_{k-1} & \dots & S_0 \\ S_k & S_k & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2k-2} & S_{2k-3} & \dots & S_{k-1} \end{bmatrix}$  is invertible then  $\begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_k \end{bmatrix}$  is unique.

### Proposition

We put for  $i = 0, 1, \dots, 2^m - 2$ ,  $S_i = \sum_{j=1}^n v_j \alpha_j^i$  and

$$\sigma(x) = \sum_{j=0}^k \sigma_j x^{k-j} \text{ and}$$

$$Q(x) = S_{2^m-2} + S_{2^m-3}x + \dots + S_1x^{2^m-3} + S_0x^{2^m-2}$$

$$\begin{bmatrix} S_{2^m-2} & S_{2^m-3} & \dots & S_0 \\ S_0 & S_{2^m-2} & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2^m-3} & S_{2^m-4} & \dots & S_{2^m-2} \end{bmatrix} \begin{bmatrix} 0 \\ \dots \\ 0 \\ 1 \\ \sigma_1 \\ \dots \\ \sigma_k \end{bmatrix} = 0 \Leftrightarrow Q(\alpha^i)\sigma(\alpha^i) = 0$$

$$; \forall i = 1, \dots, 2^m - 2$$

### Proof

By lemma 4 it was

$$\begin{bmatrix} S_{2^m-2} & S_{2^m-3} & \dots & S_0 \\ S_0 & S_{2^m-2} & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2^m-3} & S_{2^m-4} & \dots & S_{2^m-2} \end{bmatrix} \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha & \dots & \alpha^{2^m-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2^m-3} & \dots & \alpha^{(2^m-2)(2^m-2)} \end{bmatrix} \begin{bmatrix} Q(0) \\ Q(\alpha) \\ \vdots \\ Q(\alpha^{2^m-2}) \end{bmatrix} \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha^{2^m-2} & \dots & \alpha \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{(2^m-2)(2^m-2)} & \dots & \alpha^{(2^m-2)} \end{bmatrix}$$

With  $Q(x) = S_{2^m-2} + S_{2^m-3}x + \dots + S_1x^{2^m-3} + S_0x^{2^m-2}$

We will

$$\begin{bmatrix} S_{2^m-2} & S_{2^m-3} & \dots & S_0 \\ S_0 & S_{2^m-2} & \dots & S_1 \\ \dots & \dots & \dots & \dots \\ S_{2^m-3} & S_{2^m-4} & \dots & S_{2^m-2} \end{bmatrix} \begin{bmatrix} 0 \\ \dots \\ 0 \\ 1 \\ \sigma_1 \\ \dots \\ \sigma_k \end{bmatrix} = P \begin{bmatrix} Q(0) \\ Q(\alpha) \\ \vdots \\ Q(\alpha^{2^m-2}) \end{bmatrix} P^{-1} \begin{bmatrix} 0 \\ \dots \\ 0 \\ 1 \\ \sigma_1 \\ \dots \\ \sigma_k \end{bmatrix} \text{ therefore}$$

$$C_s \begin{bmatrix} 0 \\ \dots \\ 0 \\ 1 \\ \sigma_1 \\ \dots \\ \sigma_k \end{bmatrix} = 0 \Leftrightarrow \begin{bmatrix} Q(0) \\ Q(\alpha) \\ \vdots \\ Q(\alpha^{2^m-2}) \end{bmatrix} \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \alpha^{2^m-2} & \dots & \alpha \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{(2^m-2)(2^m-2)} & \dots & \alpha^{(2^m-2)} \end{bmatrix} \begin{bmatrix} 0 \\ \dots \\ 0 \\ 1 \\ \sigma_1 \\ \dots \\ \sigma_k \end{bmatrix} = 0$$

$$\Leftrightarrow \begin{bmatrix} Q(0) \\ Q(\alpha) \\ \vdots \\ Q(\alpha^{2^m-2}) \end{bmatrix} \begin{bmatrix} \sigma_k + \dots + \sigma_1 + 1 \\ \sigma_k \alpha + \sigma_{k-1} \alpha^2 + \dots + \sigma_1 \alpha^k + 1 \\ \vdots \\ \sigma_1 \alpha^{2^m-2} + \sigma_{k-1} \alpha^{(2^m-2)} + \dots + \sigma_1 \alpha^{k(2^m-2)} + 1 \end{bmatrix} = 0$$

$$\Leftrightarrow \begin{bmatrix} Q(0)\sigma(0) \\ Q(\alpha)\sigma(\alpha) \\ \vdots \\ Q(\alpha^{2^m-2})\sigma(\alpha^{2^m-2}) \end{bmatrix} = 0 \Leftrightarrow Q(\alpha^i)\sigma(\alpha^i) = 0$$

for all  $i = 0, 1, \dots, 2^m - 2$

### Proposition

We put for  $i = 0, 1, \dots, 2^m - 2$ ,  $S_i = \sum_{j=1}^n v_j \alpha_j^i$  and

$$\sigma(x) = \sum_{j=0}^k \sigma_j x^{k-j} \text{ and}$$

$$Q(x) = S_{2^m-2} + S_{2^m-3}x + \dots + S_1x^{2^m-3} + S_0x^{2^m-2}$$

$$\{i, \sigma(\alpha^i) = 0\} = \{i, Q(\alpha^i) \neq 0\} = k \text{ and}$$

$$Q(\alpha^i) \neq 0 \Leftrightarrow \sigma(\alpha^i) = 0$$

### Proof

By the previous proposal it was

$$Q(\alpha^i)\sigma(\alpha^i) = 0 ; \forall i = 1, \dots, 2^m - 2 \text{ therefore if}$$

$$Q(\alpha^i) \neq 0 \text{ we will } \sigma(\alpha^i) = 0 \text{ then}$$

$$\{i, Q(\alpha^i) \neq 0\} \subset \{i, \sigma(\alpha^i) = 0\} \text{ gold}$$

$$\text{card}\{i, Q(\alpha^i) \neq 0\} = \text{rg} C_s = k \text{ and}$$

$$\text{card}\{i, \sigma(\alpha^i) = 0\} = k$$

## VIII – Our decoding algorithm

The syndrome vector all received word not exceeding the correction capacity is calculated by simple matrix product control word received by the. We still have to find a method to calculate the extended syndromes. We must convert each element of  $F_{2^m}$  a column vector  $m$  component of  $F_2$  taken

with respect to a natural base  $\{1, \alpha, \dots, \alpha^{m-1}\}$ .

Algorithm

Input :  $(S_j^\lambda)_{j=0,1,\dots,2^m-2}^{\lambda=1,\dots,m}$

Output :  $(e_1, \dots, e_n)$

$$\text{for } \lambda = 1, \dots, m \quad Q^\lambda(x) = S_{2^m-2}^\lambda + S_{2^m-3}^\lambda x + \dots + S_1^\lambda x^{2^m-3} + S_0^\lambda x^{2^m-2}$$

$$\text{for } i = 1, \dots, n \quad Q^\lambda(\alpha_i) \neq 0 \text{ these } e_i^\lambda = 1 \text{ else } e_i^\lambda = 0$$

$$\text{for } i = 1, \dots, n \quad F_{2^m}^m \rightarrow F_{2^m} \quad (e_1^1, \dots, e_i^m) \rightarrow E_i \text{ and if}$$

$$E_i = 0 \text{ then } e_i = 0 \text{ else } e_i = 1$$

## IX- Conclusion

Our approach overcomes the vulnerability of cryptosystems MC Eliece, incurred as information leakage, caused by the fact that the number of iterations in the Euclidean algorithm is influenced by the number of error bits that this cryptosystem must hide. This approach requires to find an effective method

for calculate the syndromes of extended classical irreducible Goppa codes.

#### **X- bibliographie**

- [1]: H.Gregor Molter.Marc Stottinger.Abdulhadi Shoufan.Falko Strenzke-2011 A simple power analysis attack on a McEliece cryptoprocessor
- [2]: Daniel Augot Magali Bardet Jean-charles Faugère On the decoding of binary cyclic codes with the Newton identities 2009.
- [3]: Magali Turrel Bardet Thèse de doctorat de l'université Paris 6 Etude des systemes algébriques surdeterminés. Applications aux codes correcteurs et à la cryptographie 2004.
- [4]: Houssam Khalil Matrices structures et matrices de Toeplitz par blocs de Toeplitz en calcul numérique et formel Thèse de doctorat 2008 université Claude Bernard-Lyon1
- [5]: Kequin Fenga.Lanju Xu Fred J.Hickernellb Linear error-block codes 2005
- [6]: Error-Correcting Codes and finite Fields OliverPRETZEL Imperial college lo,ndon 1992
- [7]: Quleques applications des transformations discretes de Galois-Fourier aux codes de Goppa. Jean Conan Ecole polytechnique canada 1987.

# RST-Based Analysis of Multi-Class Multi-Servers Non-Preemptive Priority Queues versus Worst Case IEEE Analysis

<sup>1</sup> Amin B. A. Mustafa, <sup>1</sup> Mohammed A. A. Elmaleeh,

<sup>1</sup> Faculty of Engineering, Alneelain University, Khartoum,  
Sudan.

<sup>1</sup> Jebra, Block16, No 433, Khartoum, Sudan.

Hassan Yousif<sup>2</sup>, Mohammed Hussein<sup>3</sup>,

<sup>2</sup> College of Engineering, EE Dept, Salman bin Abdulziz  
University, Wadi Aldwassir, KSA

<sup>3</sup> Faculty of Engineering, Sudan University of Science and  
Technology, Khartoum, Sudan

**Abstract**— In this paper, analysis of non-preemptive priority queues with multiple servers and multiple priority classes is presented. It is assumed that the service times – for all priority classes – are identically and exponentially distributed to simplify the complexity of the residual service time mathematical expression to an extent will enable calculating the average customer waiting time. The paper proposes an expression for the mean residual service time which then used in developing a mathematical model for the analysis of Pre-emptive and non-preemptive priority queues with multiple servers and multiple priority classes. This is followed by a comparative study between the proposed scheme and the Worst Case Analysis results. This could help a lot in justifying and supporting this proposed RST-Based Analysis.

**Keywords**- Non-preemptive; Multiple Servers; Mathematical Model

## I. INTRODUCTION

One of the most powerful mathematical tools for making quantitative analysis of computer networks and communication systems is the queuing theory [1]. Analytical techniques based on queuing theory provide a reasonably good fit to reality. They may play a very important role in studying the effect of load changes, forming a good base for design purposes and for making necessary performance projections. To characterize computer communication networks performance the average delay required to deliver a packet (a message) from origin to destination is measured or calculated. Delay considerations have a strong influence on the choice and performance of network routing, flow control and congestion control algorithms [2-3].

In computer networks, there are several models describing the behavior of both preemptive and non-preemptive queuing systems. In the non-preemptive queuing systems, it is assumed that always the highest priority job is selected by the server with no interruptions allowed until the job is completed. On the other hand, in the preemptive queuing systems, models allow job interruption if a higher priority job is submitted. In this paper we will focus our discussion on the non-preemptive priority queuing systems [4].

Several researchers have treated delays encountered by jobs on non-preemptive priority queuing systems where only limited number of priority classes is considered. D. Lee and G. Horvath have considered non-preemptive queuing systems with two priority classes namely high and low-priority. Moreover, Landry and Stavrakakis have developed a three-priority queuing policy that can be applied to the distributed queue dual bus (DQDB) [6]. Multiple priority classes are rarely discussed in literature. Developing a generalized model for waiting time for multi-class multi-server systems would be critically needed to design newer networks where multiple priority classes can be implemented. In this paper, multiple priority classes are considered during the calculations of delays encountered by jobs using multiple servers, non-preemptive systems. The use of queuing theory often requires making simplifying assumptions to perform meaningful yet close to reality analysis. In general more realistic assumptions result in highly complex analytical expressions which tender an extremely difficult analysis. It is sometimes impossible to obtain accurate quantitative delay predictions on the basis of queuing models that make use of very realistic assumptions [5-7].

The paper is organized as follows. In Section II a background for priority queuing systems where the wait time for each priority class with one server is derived. The derived relation for the wait time is then expanded to multiple servers' case as will be shown in Section III. A numerical examples and results discussion are given in Section IV. In section V, case analysis of comparing RST of non-preemptive priority queues with worst J is given. In Section VI the conclusions are presented.

## II. BACKGROUND FOR PRIORITY QUEUING SYSTEMS

The analysis of Priority Queuing is based on the analysis of M/G/1 system in which customers arrival rate follows a Poisson Process with rate  $\lambda$  and the customers service times have a general distribution ( M stands for memory less systems). In priority queuing systems the arriving customers are divided into n priority classes such that for class k, the priority of class k where  $0 < k < n$  is higher than priority of class k+1 [8].

The arrival rate and the first two moments of service times of each priority class are denoted as:

$$\lambda_k, \overline{x_k} = \frac{1}{\mu_k} \text{ \& } \overline{x_k^2} \quad (1)$$

Arrivals of all classes are assumed to be independent, Poisson and independent of the service times.

Non-preemptive priority rule dictates that a customer undergoing service is allowed to complete service without being interrupted.

To determine the average delay for each priority class, the following parameters are defined according to the standard notation in [7]:

$N_Q^k \equiv$  Average number in queue for priority class k

$W_k \equiv$  Average queuing time for priority class k

$\rho_k = \frac{\lambda_k}{\mu_k} \equiv$  System utilization for priority class k

$R \equiv$  Mean residual service time

The overall system utilization is less than unity. Then

$$\rho_1 + \rho_2 + \rho_3 + \dots + \rho_n \quad (2)$$

The customer waiting time  $w$ , is composed of two components:

- I. The mean residual service time  $R$  which is the time required to complete the service of the undergoing service customer.
- II. The time required for the service of all queued customers.

The system service rate is  $\mu$  then average service time of a given customer is  $1/\mu$  assuming that there are  $N_Q$  queued customers in the system, then the total service time for all customers is

$$\frac{N_Q}{\mu} \quad (3)$$

Then the total wait time can be given by:

$$W = R + \frac{N_Q}{\mu} \quad (4)$$

Applying (4) for the highest priority class

$$W_1 = R + \frac{N_Q^1}{\mu_1} \quad (5)$$

From Little's Theorem, it is known that

$$N = \lambda W \quad (6)$$

where  $\lambda$  is the average customers' arrival rate. Considering the highest priority class, expression (5) becomes

$$\frac{N_Q^1}{\mu_1} = \lambda W_1 \quad (6)$$

Using expression (6) in equation (4), the first priority waiting time can be described as

$$W_1 = \frac{R}{(1 - \rho_1)} \quad (7)$$

where  $\rho$  is the utilization factor, which is defined as the ratio of the average customers' arrival rate to the average service rate

$$\rho = \frac{\lambda}{\mu} \quad (8)$$

There is a similar expression for the second priority class except that, there is additional delay due to high priority customers that arrive while this second priority class customer is waiting in a queue. This additional delay should be taken into account. Then  $W_2$  is given by

$$W_2 = R + \frac{N_Q^1}{\mu_1} + \frac{N_Q^2}{\mu_2} + \lambda_1 \frac{W_2}{\mu_1} \quad (9)$$

Rearranging and using Little's Theorem, the waiting time for the second priority class becomes:

$$W_2 = \frac{R + \rho_1 W_1}{1 - \rho_1 - \rho_2} = \frac{R}{(1 - \rho_1 - \rho_2)(1 - \rho_1)} \quad (10)$$

Intuitively, for any priority class k,  $W_k$ , can be given by

$$W_k = \frac{R}{(1 - \rho_1 \dots \rho_k)(1 - \rho_1 \dots \rho_{k-1})} \quad (11)$$

The average delay per customer of class k is composed of two components, the service time plus the waiting time (Queuing time). Then the average delay  $T_k$  is given by:

$$T_k = \frac{1}{\mu} + W_k \quad (12)$$

It can be shown that, the residual service time in single server systems, is given by:

$$R = \frac{1}{2} \sum_{i=1}^n \lambda_i \overline{x_i^2} \quad (13)$$

### III. EXTENSION TO MULTIPLE SERVERS CASE

The above formula cannot be extended to multiple servers' case (multiple communication channels from the communication systems point of view) due to the fact that, the residual service time is complex to formulate mathematically

in a fashion simple enough to enable calculating the average customer waiting time. To overcome this problem, the proposed solution is to assume that the service times for all priority classes are identically and exponentially distributed.

Consider the M/M/m system in which customers arrive according to a Poisson process while service times are exponentially distributed, it can be shown that, using Markov Chains, the probability of n customers in the system is given by:

$$p_n = p_0 \frac{(m\rho)^n}{n!} \quad (14)$$

$n \leq m$

$$p_n = p_0 \frac{m^m \rho^n}{m!} \quad (15)$$

$n > m$

where  $\rho$  is the utilization factor, m is the number of servers (Communication Channels),  $p_0$  is the probability of 0 customers in the system.

Since

$$\sum_{n=0}^{\infty} p_n = 1$$

Then using (14) and (15), one can write  $p_0$  as follows:

$$p_0 = \left[ 1 + \sum_{n=1}^{m-1} \frac{(m\rho)^n}{n!} + \sum_{n=m}^{\infty} \left( \frac{(m\rho)^n}{m!} * \frac{1}{m^{n-m}} \right) \right]^{-1} \quad (16)$$

The first term on the left side of (16) can be simplified to

$$1 + \sum_{n=1}^{m-1} \frac{(m\rho)^n}{n!} = \sum_{n=0}^{m-1} \frac{(m\rho)^n}{n!}$$

And the second term on the left side of (16) can be simplified to

$$\sum_{n=m}^{\infty} \left( \frac{(m\rho)^n}{m!} * \frac{1}{m^{n-m}} \right) = \frac{m^m}{m!} \frac{\rho^m}{(1-\rho)}$$

Then (16) becomes:

$$p_0 = \left[ \sum_{n=0}^{m-1} \frac{(m\rho)^n}{n!} + \frac{m^m}{m!} \frac{\rho^m}{(1-\rho)} \right]^{-1} \quad (17)$$

The queuing probability is the probability that an arrival will find all servers busy and hence it will be forced to wait in a queue. This probability gives a powerful measure for the evaluation of the performance of different communication systems. Equation (17) shows that, the queuing probability  $P_Q$  is given by:

$$P_Q = \sum_{n=m}^{\infty} p_n = p_0 \frac{m^m}{m!} \frac{\rho^m}{(1-\rho)} \quad (18)$$

where  $P_0$  is given by Equation (17). The expected number of customers waiting in queue (not in service) is given by:

$$N_Q = \sum_{n=0}^{\infty} n * p_{m+n} \quad (19)$$

Since

$$E(x) = \sum_{\text{for all } i} x_i * f(x_i)$$

Equation (25) states:

$$p_n = p_0 \frac{m^m \rho^n}{m!}$$

Then

$$p_{m+n} = \frac{m^m \rho^{m+n}}{m!}$$

Then after few mathematical manipulations,  $N_Q$  can be shown to be:

$$N_Q = \sum_{n=0}^{\infty} n p_0 \frac{m^m \rho^{m+n}}{m!} = p_0 \frac{(m\rho)^m}{m!} \rho * \frac{1}{(1-\rho)^2}$$

From the expression of  $P_Q$  given in (20),  $P_0$  can be written as

$$p_0 = \frac{P_Q * m! (1-\rho)}{(m * \rho)^m} \quad (20)$$

I. Substituting for  $P_0$  in (20) and simplifying,  $N_Q$  can be written as

$$N_Q = P_Q \frac{\rho}{(1-\rho)}$$

By using Little's Theorem in (5), then the average time  $W$  the customer has to wait in queue can then be given by:

$$W = \frac{\rho * P_Q}{\lambda (1 - \rho)} \quad (21)$$

The utilization factor  $\rho$  for a given priority class  $i$  is given by

$$\rho_i = \frac{\lambda_i}{m\mu} \quad (22)$$

$$\rho = \sum_{i=1}^n \rho_i \quad (23)$$

From equation (7), (22), (23), the residual service time  $R$  can be written as

$$R = \frac{P_Q}{m\mu} \quad (24)$$

Equation (24) can be used in the calculation of the customer waiting time, in multiple servers' non-preemptive queuing systems as follows:

Substituting (24) in (11) gives:

$$W_k = \frac{P_Q / m\mu}{(1-\rho_1-\rho_2-\dots-\rho_{k-1})(1-\rho_1-\rho_2-\dots-\rho_k)} \quad (25)$$

where  $P_0$  and  $P_Q$  are given by (17) and (18) respectively.

#### IV. NUMERICAL DEMONSTRATION AND DISCUSSION

The above detailed equations that describe the customer waiting times for different priority classes in multiple servers (multiple communication channels) non-preemptive priority queuing systems, were used in writing a simple computer simulation program. Specifying the required parameters and inputs, the simulation program was used in obtaining waiting times corresponding to different priority classes as described by Equation (25).

The first run of the simulation program assumes the following set of values for different parameters:

Number of servers - communication channels:  $m=8$

Number of priority classes:  $k=10$

Utilization factors for all priority classes:  $\rho_i = 0.085$  ( $1 \leq i \leq 10$ )

System service rate per server -communication channel-:  $\mu = 16$

The second execution of the simulation program applies similar set of values used in the previous test for different

parameters. The system service rate per server namely the communication channel is given by:  $\mu = 4$ .

The results representing waiting times for different priority classes are shown in Table1. The results presented in Table 1 are plotted as shown in Figure 1

Table 2 symbolizes the results of the waiting times for different priority classes. The results presented in Table 2 are plotted as shown in Figure 2. Accordingly, the results representing waiting times for different priority classes are shown in Table1.

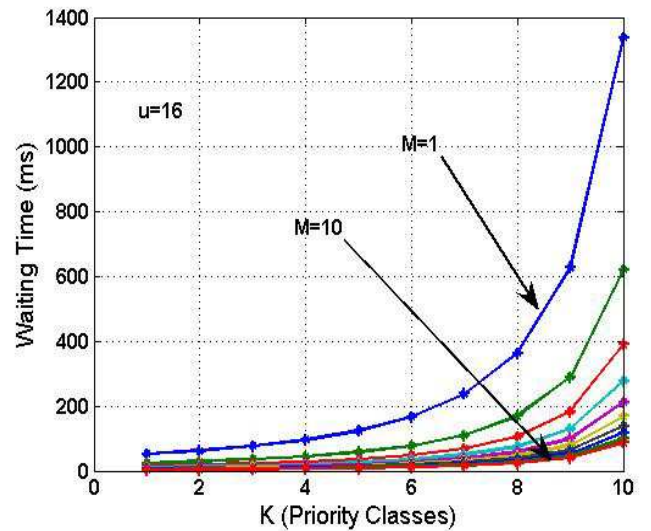


Figure 1. Waiting times vs. Priority classes for multi-servers for U=16

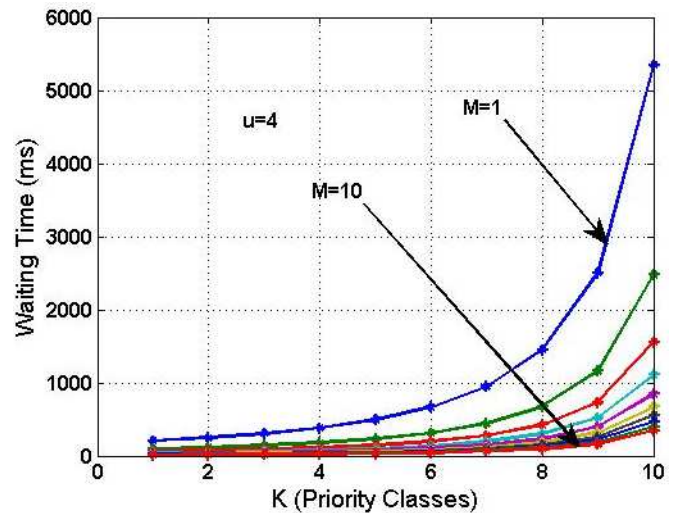


Figure 2. Waiting times Vs Priority classes for multi-servers for U=4

#### V. CASE ANALYSIS COMPARISON OF RST ANALYSIS OF NON-PREEMPTIVE PRIORITY QUEUES WITH WORST J.

Schmitt has derived worst case bounds on delay and backlog for non-preemptive priority queuing systems [9]. He utilized

the results of the average behavior of non-preemptive priority queuing systems obtained from traditional queuing theory in addition to some numerical investigations to compare the worst case bounds to those average behavior results. Schmitt has compared worst case bounds to average behavior results in

order to give a feel as to how conservative the worst case bounds are. Practical implications of such results cover different networks which use simple priority queuing to differentiate between several traffic classes by assigning them different delay targets.

TABLE I. WAITING TIMES FOR DIFFERENT PRIORITY CLASSES AND SERVERS WITH  $U=16$ .

W (m sec)										
M K	1	2	3	4	5	6	7	8	9	10
1	0.0515	0.0239	0.0150	0.0107	0.0081	0.0065	0.0053	0.0045	0.0039	0.0034
2	0.0620	0.0288	0.0181	0.0129	0.0098	0.0078	0.0064	0.0054	0.0046	0.0040
3	0.0762	0.0353	0.0222	0.0158	0.0120	0.0096	0.0079	0.0067	0.0057	0.0050
4	0.0958	0.0444	0.0279	0.0199	0.0152	0.0121	0.0099	0.0084	0.0072	0.0062
5	0.1242	0.0576	0.0361	0.0257	0.0196	0.0157	0.0129	0.0109	0.0093	0.0081
6	0.1672	0.0775	0.0487	0.0346	0.0264	0.0211	0.0174	0.0146	0.0125	0.0109
7	0.2374	0.1101	0.0691	0.0492	0.0375	0.0300	0.0247	0.0208	0.0178	0.0155
8	0.3636	0.1686	0.1058	0.0753	0.0575	0.0459	0.0377	0.0318	0.0272	0.0237
9	0.6266	0.2905	0.1824	0.1298	0.0991	0.0790	0.0651	0.0548	0.0469	0.0408
10	1.3367	0.6198	0.3890	0.2769	0.2113	0.1686	0.1388	0.1169	0.1001	0.0870
U=16										

TABLE II. WAITING TIMES FOR DIFFERENT PRIORITY CLASSES AND SERVERS WITH  $U=4$

W (m sec)										
M K	1	2	3	4	5	6	7	8	9	10
1	0.2060	0.0955	0.0600	0.0427	0.0326	0.0260	0.0214	0.0180	0.0154	0.0134
2	0.2482	0.1151	0.0722	0.0514	0.0392	0.0313	0.0258	0.0217	0.0186	0.0162
3	0.3048	0.1413	0.0887	0.0631	0.0482	0.0385	0.0316	0.0266	0.0228	0.0198
4	0.3833	0.1777	0.1116	0.0794	0.0606	0.0484	0.0398	0.0335	0.0287	0.0250
5	0.4966	0.2303	0.1445	0.1029	0.0785	0.0627	0.0516	0.0434	0.0372	0.0323
6	0.6689	0.3102	0.1947	0.1386	0.1058	0.0844	0.0695	0.0585	0.0501	0.0436
7	0.9497	0.4404	0.2764	0.1968	0.1502	0.1198	0.0986	0.0830	0.0712	0.0618
8	1.4542	0.6743	0.4233	0.3013	0.2299	0.1835	0.1510	0.1271	0.1090	0.0947
9	2.5063	1.1622	0.7295	0.5192	0.3963	0.3162	0.2602	0.2191	0.1878	0.1632
10	5.3467	2.4793	1.5562	1.1077	0.8453	0.6745	0.5551	0.4674	0.4006	0.3481
U=4										

The contributions of Schmitt's work include the derivation of results for the worst case behavior in non-preemptive priority queuing systems. This extends to cover the derivation of the service curves for each traffic class.

Additional worth mentioning contribution is the derivation of the results based on the service curves bounds on delay and buffer requirements for each class. Practical implications from Schmitt's work apart from the fundamental insights from the comparison of average and worst case behavior are in network performance control. This means that, the obtained results can be applied for admission control purposes to achieve certain delay targets in each traffic class.

Worst case analysis is based on M/G/1 system. The numerical examples presented by J. Schmitt cover the average and the worst case delays for different priority classes and different server capacities. The corresponding plots illustrate the relations between the above stated parameters.

As expected, it is found that Schmitt's plots describing the relation between worst case and average delays Vs priority classes, see Figures 3 and 4, are very similar to the plots describing the behavior of the Multi-class Multi-servers non-preemptive priority queuing systems as shown in Figures 1 and 2.

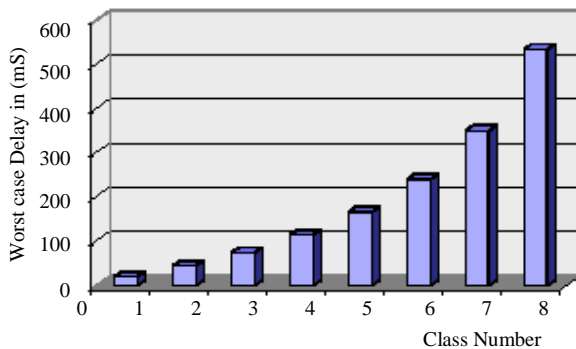


Figure 3. Worst Case Delay for Different Priority Classes (According to Schmitt)[9]

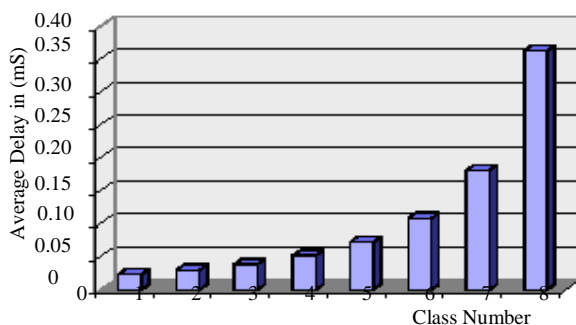


Figure 4. Average delay for different priority classes (According to Schmitt) [9]

Figure 5 and 6 illustrate the relation between waiting times and priority classes for different number of servers in a similar

manner to that used in Figure 3 and 4 this ease the comparison procedure.

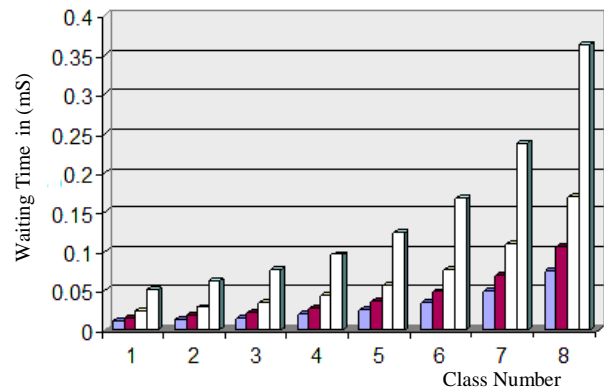


Figure 5. Waiting Times for Different Number of Servers versus Different Priority Classes

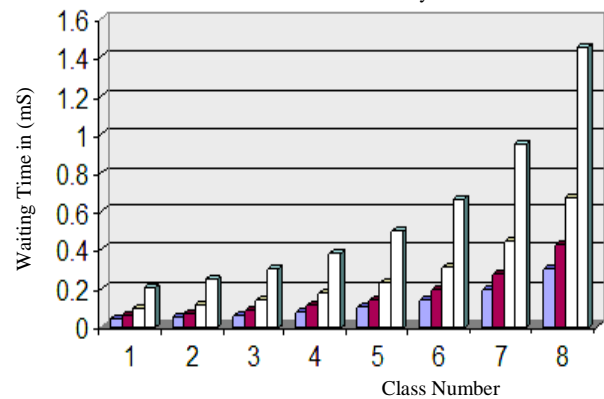


Figure 6. Waiting Times for Different Number of Servers versus Different Priority Classes

Furthermore, the plots describing the relation between average and worst case delays versus different server capacities are very similar to their counter parts describing the relation between average waiting time versus number of servers. This is expected due to the fact that, the increased server capacity sounds the same as increasing number of servers. This relation is shown in Figure 7 and Figure

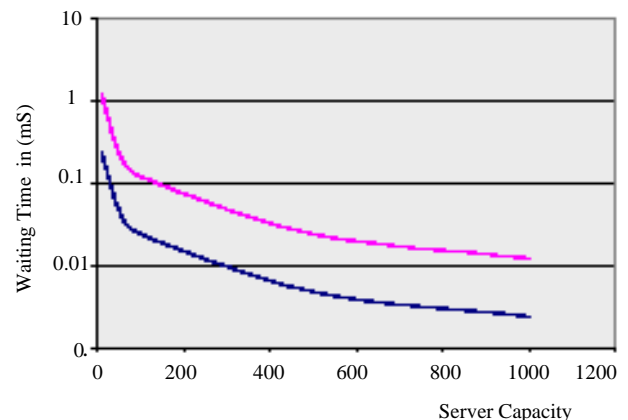


Figure 7. Average Delay for Different Server Capacities



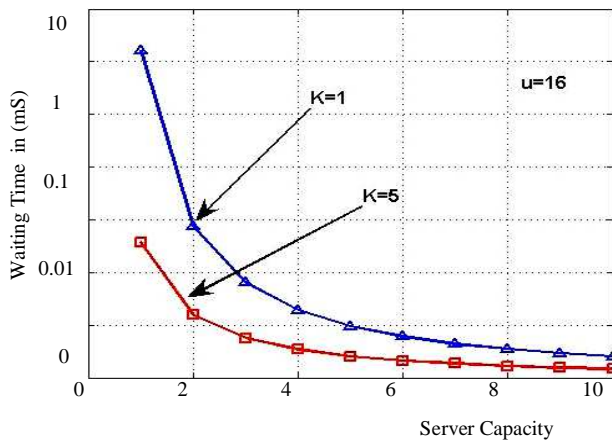


Figure 8. Waiting Time Versus Number of servers for different priority classes with  $U=16$

## VI. CONCLUSIONS

The assumption that the service times for all priority classes are identically and exponentially distributed led to the possibility of extending the analysis of non-preemptive priority queuing systems to the multiple servers case (multiple communication channels). The extension is based on the developed formula for the residual service time  $R$ . This was achieved by utilizing the analysis of  $M/M/m$  systems in which the service times are identically and exponentially distributed, combining this with the analysis of non-preemptive queuing systems for single server systems based on  $M/G/1$  system and making the necessary modifications for the system to fit the multiple servers case. Starting from well-known relations, all the necessary mathematical relations were shown. The extended relations were used in estimating wait time for systems with multiple priority classes and servers. Results of extended model agrees with published wait time trends.

The discussion presented by section IV shows that, most analysis concerning non-preemptive systems are dealing with restricted number of priority classes in particular, two priority classes. This is coupled with the fact that, most of these systems deal with a single server.

Another worth mentioning point is that, most of the presented scenarios are based on simplifying assumptions. Consequently, the obtained results are restricted, from accuracy point of view, to the applied simplifying assumptions.

An additional point is that, some of these scenarios are dedicated to special systems and special areas of applications. An example is S. Ghani and M Schwartz analysis that deals with the performance evaluation of non-preemptive priority in GSM systems which is dedicated for GSM systems.

The above mentioned points justify that, the proposed scheme is characterized by its generality, accuracy and applicability. The comparison between the proposed analysis and the analysis done by J. Schmitt [9] covering worst case analysis, shows their agreement as the results obtained in both cases are very similar despite that, the latter is only a special case for one server. The plots describing average and worst case delays Vs different server capacities in Schmitt's paper are very similar to their counterparts of the proposed system describing the relation between average waiting time Vs number of servers. Again, this justifies the claim that, the results obtained by the proposed system agrees with another different approach proposed by Schmitt.

## REFERENCES

- [1] Tanen, A, Computer Networks, 3rd ed. Prentice Hall of India, New Delhi, 1996.
- [2] Stalling, W, High Speed Networks, Prentice Hall, Upper Saddle River. New Jersey, 1998.
- [3] Enns, S. T. and Sangjin Choi, "Use of GI/G/1 Queuing Approximation to test tactical parameters for the simulation of MRP systems", Simulation Conference, 2002. Proceedings of the Winter Volume, vol. 2, pp. 1123 – 1129, Dec. 2002.
- [4] Duan-Shin Lee, "A generalized non-preemptive priority queue", INFOCOM '95. Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Bringing Information to People. Proceedings, vol. 1, pp. 354 – 360, April 1995
- [5] Gabor Horvath, "A Fast Matrix-Analytic Approximation for the Two Class GI/G/1, Non-Preemptive Priority Queue", 12th International conference on analytical and stochastic modelling Techniques and Applications ASMTA 2005 in Conjunction with 19th European Conference on Modelling and Simulation, June 2005.
- [6] Randall Landry and Ioannis Stavrakakis, "Queuing study of 3-priority policy with distinct service strategies", IEEE/ACM Trans. on Networking, vol.1, pp. 576-589, October 1993.
- [7] Bertsekas, D. & Gallger, R, Data Networks, Prentice Hall Engle wood cliffs, New Jersey, 1992.
- [8] Silva, F. & Serra, D. 2003, "Locating Emergency Services with priority rules: The priority Queuing Location Problem", 27th Conference of National Statistics and Investigational Operations.
- [9] Jens Schmitt, "On average and Worst Case Behavior in Non-Preemptive Priority Queuing" Darmstadt University of Technology, 2001.

## AUTHORS PROFILE



Amin B. A. Mustafa received his BSc degree in electrical engineering, University of Khartoum, Sudan. He works in NARIS, Sudan, as communication and computer networking engineer for a coupled of years. In 1996 Mr Amin received his MSc degree in computer engineering. He joined Hadhramout university, Yaman for five years. In 2008 Dr Amin received his PhD Degree in Computer Engineering and Networking. Since then Dr Amin supervised

many post graduate students in their research projects. His research interest includes wireless communication and computer engineering..



Mohammed Elmaleeh received his BSC degree from University of Gezira (Sudan), Faculty of Engineering and Technology (Communication and Control Engineering). In 1998 Elmaleeh received his MSc in Electrical Engineering, University of Khartoum, Sudan. From 1994-1998 he worked as a researcher in Sudan Atomic Energy Commission. In 1999 Mr Elmaleeh worked as automation engineer,

QAPCO, Qatar. In 2009 Elmaleeh received his PhD degree in Electrical and Electronic Engineering, University Technology PETRONAS, Malaysia. Currently Elmaleeh works as Ass. Prof. (Sudan). He supervises PhD, MSc and FYP students in their research projects. Mr Elmaleeh is assigned as a reviewer for many IEEE conferences and international journals. His research interest includes embedded systems, control, communication and electronic engineering.



Hassan Yousif Ahmed is an Assistant Professor in Network and Communication Engineering Department at the University of King Khalid, Abha, KSA. He holds PhD degree in Electrical and Electronics Engineering from University Technology Petronas, Malaysia, 2010 in addition to Data Communication Diploma and membership of IEEE. His research interests are on Computer

Network, wireless communications networks, and optical communications.



Mohamed Hussien Mohamed Nerma (mohamed\_hussien@ieee.org) received his Ph.D. degree in communication engineering from Universiti Teknologi PETRONAS, Malaysia in 2010. He is a reviewer and invited reviewer of different international journals and conferences and he is also an active member in all assessment and accreditation activities. His research is focused on Wireless Com-munication, OFDM (WiMAX,

WiFi, DVB-T, and LTE), Cognitive radio, OFDM and FPGA, Wavelet Based OFDM Systems, and Optical Fiber Transceivers. Currently he is working for Sudan University of Science and Engineering, Khartoum, Sudan. He is a senior member of IEEE.

# Constructing Server-Clustering System with Web Services Based on Linux

Dr. Dhuha Basheer Abdullah Albazaz  
Head of Computer Sciences Dept.  
College of Mathematics and Computer sciences  
University of Mosul- Iraq

Abdulnasir Younis Ahmad  
Computer Sciences Dept.  
College of Mathematics and Computer sciences  
University of Mosul- Iraq

**Abstract**—This paper suggests a system that presents a high performance computing service across the internet. The system provides the ability of executing any parallel program by sending it from the client to be executed on the server. The ability of executing a wide range of programs is because of excluding the client-server system on only transferring files between client and server, while the responsibility of writing the source code, providing data, compiling and executing operations sequence are all assigned to the user and provided as input to the client side program. Web service technique is used in constructing the system for its high flexibility, and the ability of using it on different platforms. On the server side, translation and execution of parallel programs occurs by a Rocks cluster under the Linux-based CentOS operating system. Transferring files across the Internet was performed by using AXIOM objects that are included in Axis2 libraries.

**Keywords:** Cluster, web service, SOAP, Client, Server

## I. INTRODUCTION

Computing needs of users in last years expanded from simple short time execution programs to high time consuming programs. The emerging of the parallel systems solved the problem. Parallel systems were very expensive that it is not economic for individuals or even small foundations to own. As a supposed solution is to provide the parallel system as a service and make it available to great number of users. Providing such a system requires combining a set of techniques; distributed systems, clustering, and web services.

### A. Distributed System

Distributed systems can be defined as a collection of independent computers that appear to its users as a single coherent system. [1][2]

The result of CPU and network technology developments since the mid-1980 was the emerging of distributed systems in contrast to centralized systems (or single processor system) consisting of a single computer, its peripheral, and perhaps some remote terminals. [1]

One important characteristics of distributed system is that it hides the differences between the various computers and the ways in which they communicate. The other is to allow a consistent and uniform way of interaction for user and applications to the distributed system. It should also has the ability to expand, scale easily, continuously available. [1]. It is also characterized in that it does not have common physical clock, shared memory, Autonomous, heterogeneous and it is separated geographically [2]

### B. The Client-Server Model

Processes in distributed systems are organized in terms of clients that request services from servers. A *client* is a process that requests a service from a server by sending it a request and subsequently waiting for the server reply. A *server* is a process implementing a specific service, for example, a file system service or a database service.

### C. Parallel Systems

One common and useful taxonomy of parallel processor systems[3] that characterizes the type of parallel activity by the relation of the instructions and the data is: *Single instruction single data (SISD)*, *Single instruction multiple data (SIMD)*, *Multiple instruction single data (MISD)*, and *Multiple instruction multiple data (MIMD)*

In the realm of HPC, we are for the most part dealing with MIMD systems. MIMD systems can be further divided into 2 main groups, those sharing a main memory (tightly coupled), and those that don't share memory (loosely coupled). In building computing clusters, we often make use of both of these types of MIMD architectures.[4]

Emerging of parallel computers enabled the development and deployment of grand challenging applications, such as weather forecasting and earthquake analysis[5].

#### • Characteristics of parallel systems

A parallel system may be broadly classified as belonging to one of three types [6]:

1. A multiprocessor system: A parallel system in which the multiple processors have direct access to shared memory which forms a common address space.

A multiprocessor system usually corresponds to a uniform memory access (UMA) architecture in which the access latency is the same. Inter-process communication across processors is traditionally through read and writes operations on the shared memory, although the use of message-passing primitives such as those provided by the MPI is also possible (using emulation on the shared memory). All the processors usually run the same operating system, and both the hardware and software are very tightly coupled.

2. A multicomputer parallel system: A parallel system in which the multiple processors do not have direct access to shared memory. The memory of the multiple processors may or may not form a common address space. Such computers usually do not have a common clock.

The processors communicate either via a common address space or via message-passing. A multicomputer system that has a common address space usually corresponds to a non-uniform memory access (NUMA) architecture in which the latency to access various shared memory locations from the different processors varies.

3. Array processors: Classes of parallel computers that are physically co-located, are very tightly coupled, and have a common system clock (but may not share memory and communicate by passing data using messages).

In addition to the power of parallel computers, the price performance ratio of a small cluster-based parallel computer as opposed to a minicomputer is much smaller and consequently a better value. [7]

### D. Clusters

A cluster computer is a computing platform, which consists of a collection of interconnected computers working together as a single integrated resource [2] ,[8][2]. A node of the cluster may be a single or multiprocessor computer, such as a PC, workstation, or symmetric

multiprocessor (SMP). Each node has its own memory, I/O devices and operating system. The nodes are connected via a Local Area Network (LAN) or a System Area Network (SAN) and communicate using either standard networking protocol such as TCP/IP, or a low-level protocol such as VIA.[9].

A compute cluster is used to run traditional HPC applications across the resource, parallelized applications using message passing technology, or when a large number of data sets is considered, throughput applications. It is also used to run any combination of these applications.[10]

Cluster computing provides an inexpensive computing resource to educational institutions. Colleges and universities need not invest millions of dollars to buy parallel computers for the purpose of teaching "parallel computing". A single faculty member can build a small cluster from student lab computers, obtain free software from the web, and use the cluster to teach parallel computing. Many universities all over the world, including those in developing countries, have used clusters as a platform for high performance computing.[11]

An important factor that has made the usage of clusters a practical proposition is the standardization of many of the tools and utilities used by parallel applications. Examples of these standards are the message passing library MPI and data-parallel language HPF.[2]

Cluster is a replacement of supercomputers which have very high computing performance as well as very high cost. [12] [13]. These types of clusters are also referred to as *High Performance Computing (HPC)* clusters, or simply *Compute clusters*[14]. It is not necessary that cluster machines have the same levels of performance. The only requirement for cluster machines is that they all share the same architecture. Although it is possible in theory to mix architectures when building a cluster by using Java, [15].

High-performance computing provides an invaluable role in research, product development and education. One of strength in HPC is the ability to achieve best sustained performance by driving the CPU performance towards its limits. Over the past decade, HPC has migrated from supercomputers to commodity clusters. Eighty-two percent of the Top500 HPC installations in November 2008 were clusters. [16]

Despite the fact that Computer clusters have benefits over mainframe computers that includes reduced cost, *Processing Power, Scalability, Availability* [17][18] [19], clusters have their downsides that includes great number of components, and hardness of balancing and, the need for explicitly transport data from one node to another. [14]

#### • Beowulf Cluster

One of the first known Linux-based clustering solutions is the Beowulf system [7]. Beowulf is designed for high-performance parallel computing clusters on inexpensive personal computer hardware. Beowulf systems are now deployed worldwide, chiefly in support of scientific computing.

A Beowulf cluster uses multi-computer architecture. It features a parallel computing system that consists of one or more master nodes and available compute nodes, or cluster nodes, interconnected via widely available network interconnects. All of the nodes in a typical Beowulf cluster are commodity systems- PCs, workstations, or servers- running commodity software such as Linux.

The master node acts as a server for Network File System (NFS) and as a gateway to the outside world. As an NFS server, the master node provides user file space and other common system software to the compute nodes via NFS. As a gateway, the master node allows users to gain access through it to the compute nodes. Usually, the master node is the only machine that is also connected to the outside world using a second network interface card (NIC). The sole task of the compute nodes is to execute parallel jobs. In most cases, therefore, the compute nodes do not have keyboards, mice, video cards, or monitors. All access to the client nodes is provided via remote connections from the

master node. Since compute nodes do not need to access machines outside the cluster, nor do machines outside the cluster need to access compute nodes directly, compute nodes commonly use private IP addresses, such as the 10.0.0.0/8 or 192.168.0.0/16 address ranges.[20]

One of the main differences between Beowulf and a Cluster of Workstations (COW) is the fact that Beowulf behaves more like a single machine rather than many workstations[21]

With PVM and MPI libraries and configuration tools which make the Beowulf architecture faster, easier to configure, and much more usable, one can build a Beowulf class machine using standard Linux distribution without any additional software.[22]

#### • Categories of Clusters

In general there are two broad categories of clusters:

1. Proprietary or specific systems that were preloaded and configured to work as clusters. Such systems are research machines consisting of a number of computing nodes, which are used for massively complex computations, such as weather forecasting or computational protein design. Those systems come ready or they are bundled with anything that can be used for clustering and they are based on proprietary operating systems or configurations. This category of clusters includes systems, which are usually expensive and dedicated to the specific task they are ordered for.
2. Common clusters. These clusters are built from commodity processors and memories that are used in workstations and PCs. Clusters of this category are generally classified as two main types: Beowulf class clusters and Network of Workstations (NoWs).[23]

Beowulf class clusters [24] are dedicated, high performance homogeneous clusters that are deployed when performance is the number one priority. The main feature of a Beowulf class cluster is homogeneity, i.e. all of its computing nodes are identical dedicated nodes with the exception of the "frontend computer, which allows users to submit jobs to the system. The computing nodes are dedicated to executing the processes issued by the front-end node, and usually they are not directly accessible by the users because they do not have keyboards, mice, or monitors.

NoWs are heterogeneous clusters that are designed to take advantage of otherwise "wasted computing cycles on unused computers. A master system will take job requests from authorized users, and then submit them for execution on whichever workstation has the available resources to execute them. The key difference from a Beowulf cluster is that a NOW is an heterogeneous system i.e., its computing nodes are stand alone workstations or PCs 'with -varying hardware resources and (sometimes) different architectures, connected via a communication network such as a LAN or even a WAN.[9][25]

#### • Linux Clusters

Linux is an open-source operating system like UNIX. It has the reputation of a very secure and efficient system. It is used most commonly to run network servers. It is available for wide variety of computing devices from embedded systems to huge multiprocessors, also it is available for different processors like x86, powerpc, ARM, Alpha, Sparc, MIPS, etc.[26]

Although clustering can be performed on various operating systems like Windows, Macintosh, Solaris etc.[26], Linux has its own advantages of running on a wide range of hardware. Having a wide variety of tools and applications for free, Its ability to customize the kernel for user's workload. [7], stability, free distributed code, relatively virus free, and It is a good environment for developing cluster infrastructure [26]. Linux clusters used to solve problems in specific areas such as Earth and Space science, Bioinformatics and Chemistry, and Rendering. [27]

#### • Rocks Cluster Distribution

Rocks[28] Cluster Distribution (originally called NPACI Rocks)

is a Linux distribution intended for high-performance computing clusters. Rocks was initially based on the Red Hat Linux distribution, however modern versions of Rocks are now based on CentOS, with a modified Anaconda installer that simplifies mass installation onto many computers. Rocks includes many tools (such as MPI) which are not part of CentOS but are integral components that make a group of computers into a cluster.

Installations can be customized with additional software packages at install-time by using special user-supplied CDs (called "Roll CDs"). The "Rolls" extend the system by integrating seamlessly and automatically into the management and packaging mechanisms used by base software, greatly simplifying installation and configuration of large numbers of computers.[5] Over a dozen Rolls have been created, including the SGE roll, the Condor roll, the Lustre roll, the Java roll, and the Ganglia roll.

#### E. Web Services

A web service is any service that is available over the Internet, uses a standardized XML messaging system, and is not tied to any one operating system or programming language.

There are several alternatives for XML messaging, like XML Remote Procedure Calls (XML-RPC) or SOAP. Alternatively, HTTP GET/POST could be used and arbitrary XML documents are passed. A web service may also have two additional (and desirable) properties; *self-describing* which is the public interface to the service that includes at a minimum a human-readable documentation so that other developers can more easily integrate the service, and *discoverability* which includes the availability of some simple mechanism for interested parties to find the service and locate its public interface. The exact mechanism could be via a completely decentralized system or a more logically centralized registry system.[32]

### II. RELATED WORKS

Wu *et al.* in 2002 designed a user application platform for a series of high performance computers (HPCs) via Internet (a portal). The goal of the platform is to achieve transparently accessing to any HPC, which provided in their center via Internet [30].

Shainer *et al.* in 2002 reviewed the concept of HPCaaS and Researchers explored a smart scheduling algorithm for a subset of bioscience applications in an HPCaaS system. They showed that smart scheduling can accommodate multiple applications and multiple jobs simultaneously while increasing the overall system productivity and efficiency [31].

Holmes *et al.* in 2003 aimed to the integration of standards-based web services technologies, grid-enabling software, and a component framework for parallel computing, to result in a service-oriented architecture which provides end users the ability from their desktops to manage and understand simulation results for very large, complex problems [32].

Benkner in 2005 presented the service-oriented Grid infrastructure based on standard Web Services technologies. This infrastructure automates the provision of HPC applications as Grid services for on-demand supercomputing and simplifies the construction of client-side applications [33].

Peng *et al.* in 2005 provided a Grid service that allows users to build an HPC cluster computing environment on demand and then run their applications on it. The architecture provides the basic functionality such as service deployment, service monitoring, service execution, etc. The work is useful in HPC service provisioning for Grid computing and utility computing [34].

### III. SYSTEM IMPLEMENTATION

#### A. System Overview

In this work, a proposed clustering system CTWS have been designed. CTWS system consists of two subsystems; the first is a distributed system which includes a set of clients on one side and a

server on the other side. The second is a clustering system which resides on the server side. The entire view of the system is illustrated in Fig. 1

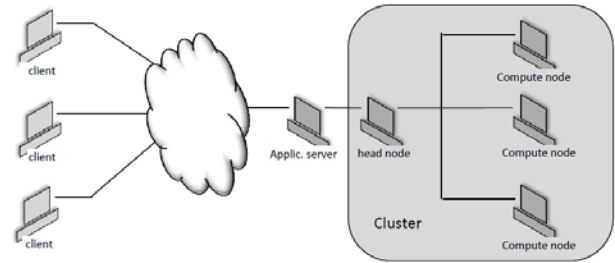


Figure 1. Entire view of the system

Client and server have been built using a Web service technology, supported by the Axis2 tool. The clustering system was built as a Beowulf cluster. Design and building the system as Web service makes it available to a large set of users. Fig. 2. Show Axis2 web service components.

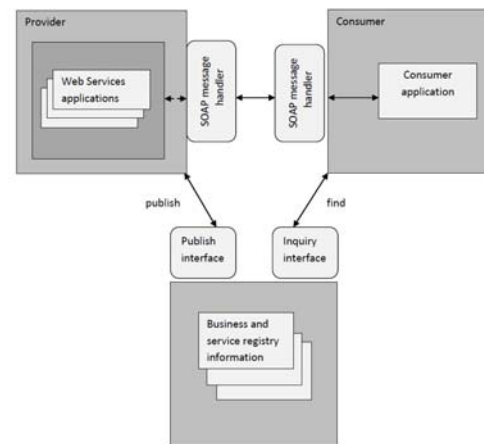


Figure 2. Axis2 Web service components

In addition to the client and server there is a registry component that the service registered by the provider to publish the service to the world, and enquired by the consumer to be enabled to call the service. For simplicity, this component is neglected from the work, supposing that the user obtains the calling information from any other resource.

The client is a module that accepts source programs (C or C++), data files-if required- and a script file as input, invokes method to upload these files to the server. Execution of the MPI program occurs on a cluster of machines that are connected to the server. The output files then, returned back to the client to be saved in a specified folder.

#### B. Client Side

On client side, three main tasks were performed: the first is the responsibility of the user. It includes preparing MPI source program, data files, and writing scripts needed for executing the program on the cluster. The user of the system proposed to be an expert user, who has knowledge in dealing with distributed computing, using cluster, and writing scripts. The second task is executing the client side of the application which responsibility is to use files produced by the user as input and invokes methods to upload these files to the server. Another task is to get the output files from the message, providing it to the user to make use of them or to look in error messages files if exists. Fig. 3. shows a block diagram for the tasks performed on the client.

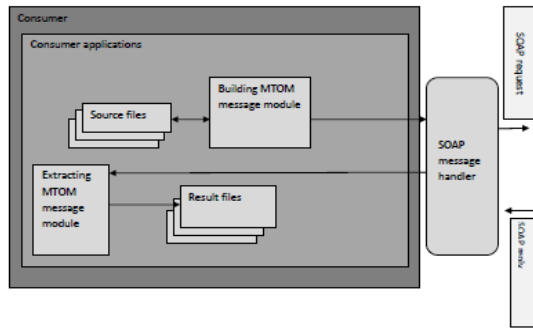


Figure 3. Client side

As SOAP messages are used to transfer data, and as these data are files which considered as large amount data, an MTOM technique was used for transferring it. In this technique the data not included in the body of the message, but it attached to the message and is pointed to by a pointer included in the message body as shown in Fig. 4. Following are a detail description of the main tasks performed by the client.

- Preparing Files

As considered before, files must be performed by the user. Two types of files were prepared. First type includes source program files, written in C or C++ as MPI programs, plus the data files (spreadsheets, multimedia ...etc).

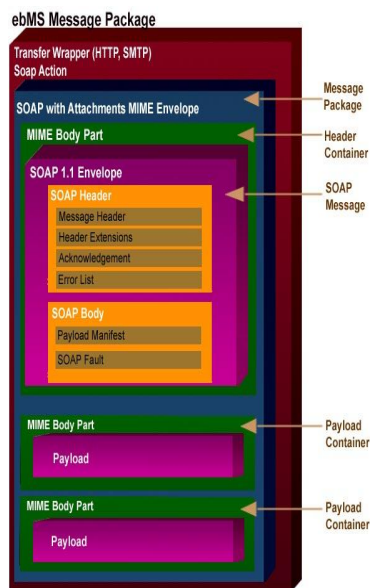


Figure 4. SOAP message

- MPI programs

Source program files supposed to be files that include MPI, or MPICH2, functions considered with parallelism, and message passing. The simplest MPI program must invoke four primary functions; MPI\_Init(), MPI\_Comm\_size(), MPI\_Comm\_rank(), MPI\_Finalize(), as illustrated in the following list in Fig. 5.

**MPI\_Init()**

This function is used to initialize the MPI program. Every statement before this function is executed on only root node.

```
#include <stdio.h>
#include <mpi.h>
int main(int argc, char *argv[]) {
    int numprocs, rank;
    MPI_Init(NULL, NULL);
    MPI_Comm_size(MPI_COMM_WORLD, &numprocs);
    MPI_Comm_rank(MPI_COMM_WORLD, &rank);

    /* This is where all the real work happens */

    MPI_Finalize();
}
```

Figure 5. Main functions of an MPI program

**MPI\_Comm\_Size()**

This function takes as input the communicator and gets the number of processes in it.

**MPI\_Comm\_rank()**

This function takes as input the communicator and gets the identifier of the machine that executes the function. As this function is executed by each node in the set, so each node gets its identifier after executing this function.

**MPI\_Finalize()**

It terminates MPI execution environment. All processes must call this routine before exiting.

For the message transferring to take place, other two functions; MPI\_Send() and MPI\_Recv() are used. The first is for sending messages and the other is for receiving it.

- Script file

The second type is the script file that contains all commands required to be executed on the cluster. These commands including configuration commands for the cluster, compile and execution commands, and are all listed in order. Fig. 6. shows a sample listing that shows a script file.

Shell that is used for receiving commands may be any shell that is available on the system. More than one shell can be installed on one system and the user can use which any of them he prefers.

```
#!/bin/bash

# To compile the program
mpicc mpi_program.c -o mpi_program

# To specify number of processes, naming the machines, and
run the program
mpirun -nolocal -np 2 -machinefile $HOME/machines \
$HOME/mpich-test/ vectormatrix
```

Figure 6. Script for main commands to execute MPI file

- Build Payload for MTOM

To set a SOAP message programmatically, first step is building the payload (body of the SOAP message) using Axis2 classes. OMElement is the essential class in building the message. The entire body is first considered as an OMElement. OMElement's could be added



as child elements, each which in turn could contain other OMElements, and so on. In this work, files to be sent; there attributes and there contents, and the folder with its name and attributes that contains these files are considered as OMElements.

Each file from the file set that to be transferred was converted to a DataHandler object. DataHandler class used to instantiate an object using a FileDataSource object as parameter. This DataHandler object used to instantiate an OMText object, to be added as child to the file OMElement. Figure(7) shows a flowchart for building SOAP message

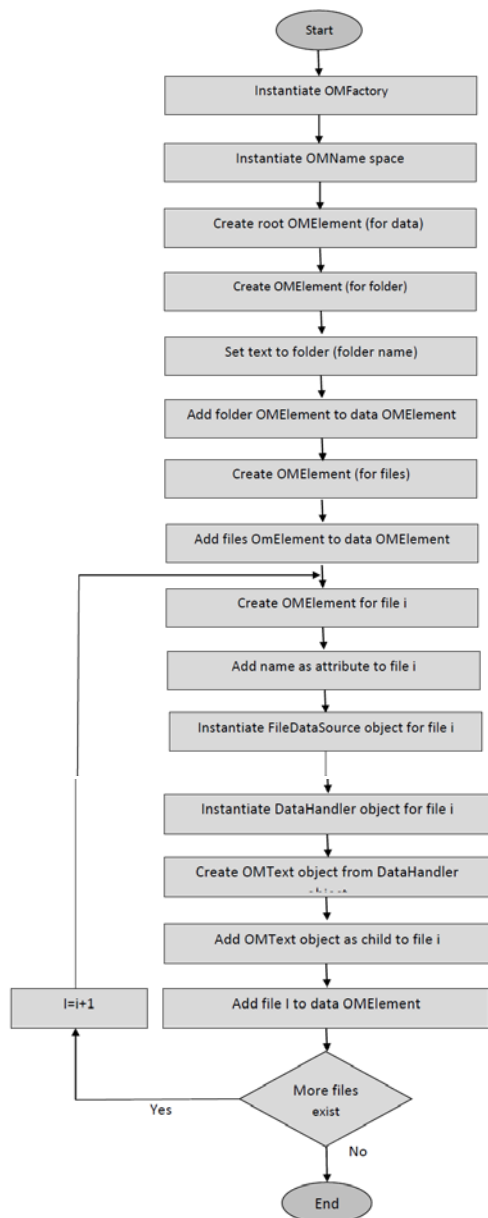


Figure 7. Steps for building SOAP message

After building payload, option and properties were set by means of Option object. A ServiceClient object then instantiated, and set to the options specified before. A ServiceClient SendRecieve() method was invoked with payload as parameter to send data (which becomes the

content of the SOAP body) to the server. Fig. 8. shows the steps of this operation.

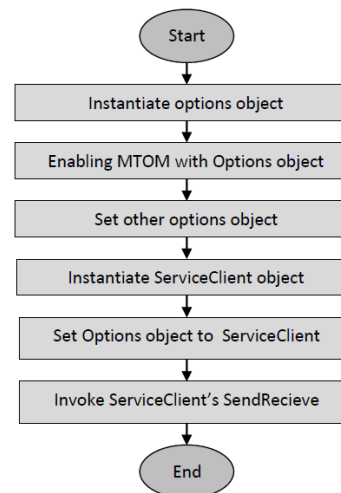


Figure 8. Prerequisite steps of invoking sendRecieve() method

#### ➤ User Interfacing

Interfacing to the system is provided on the client side program. Through the provided form, the user can choose through a visual interface the files to be sent to the service, add it to the list, clear it from the list, and finally enter the command to send files to the server.

#### • Extracting Files From Payload

After files have been returned from the server, a process of extracting them from payload was done. An Iterator object was instantiated; ChildElements were gotten, and assigned to the iterator through OMElement's getChildElements method. The iterator was traversed to extract the file name and its file data for each file. OMElement's getLocalName method was used to specify if the OMElement is for file name or for file data. The text which represents the file name is contained in an OMElement, was extracted through OMElement's getText method, and assigned to a string, while the file data was extracted through assigning the OMElement to an OMText object.

For each file, OMText's getDataHandler() method was used to get the Datahandler. DataHandler's getDatasource() method was used to get the DataSource object. Then DataSource's getInputStream method was applied to get an input stream from the file. At last a FileOutputStream object was instantiated to create an output file for each file element. A flow chart of this operation shown in Fig. 9.

#### C. Server side

Across the network, on the server side of the system, resides the server that accepts the requests. It checks it, and when it finds that is directed to Axis2 delivers it to Axis2 engine. Fig. 10. Shows server side application.

Axis2 choose the service from many services reside on it and from the operation parameter in the OMElement choose the operation to execute. Following are the modules and tasks that are attached to the server side:

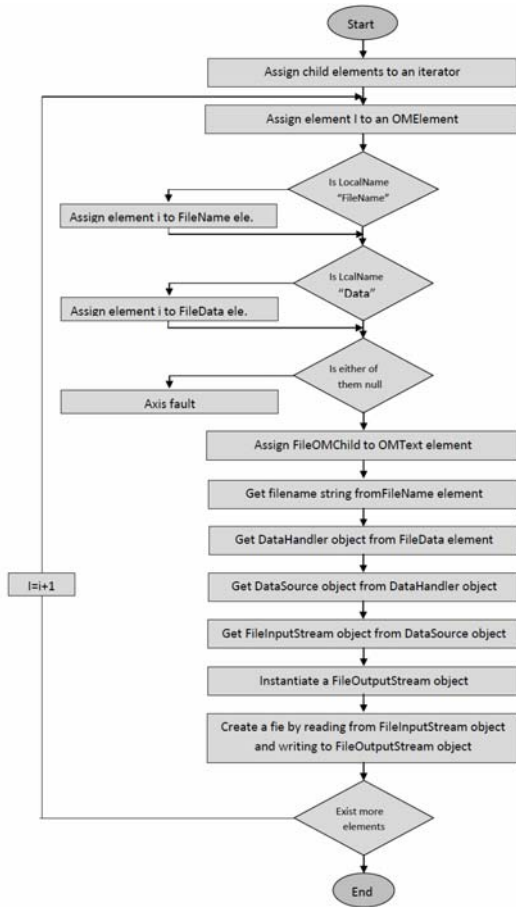


Figure 9. Extracting file data from OMElement

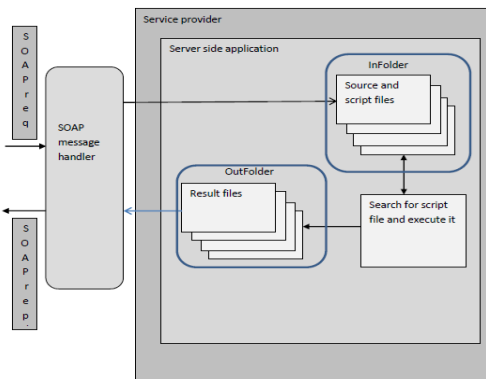


Figure 10. Server side application

#### ➤ Creating input and output folders

In function createInOutFolders(), a directory is created for the session, then an input and output folders are created in it. The input folder used as a storage for the extracted incoming files, while the output folder is used to store the output files before attaching it to the

message. The session directory is deleted as soon as its contents are transferred to the client.

#### ➤ Extract files from the message

The function extractOMEElement() extract the files included in the SOAP message and store them in the input directory.

#### ➤ Search for script file

Through the function searchForScriptFile(), the program search for the script file which contains commands for compiling and executing the program. The function send error message if the file does not exist.

#### ➤ Execute script file

After the script file had been found, It is executed through the function executeScriptFile(). Script file contains the required commands to compile and run the MPI program. Output files then stored in output folder created before.

#### ➤ Build response payload

The response is provided by the function buildResponsePayload() to be returned to the client. Operation of providing the response is as same as building payload on the client.

The server side contains a set of functions. The main function is that invoked by the client to get the files from the SOAP message. Other functions are invoked so as to prepare folders for input and output, extract files to input folders, search for script file, execute the script, and save the output files to output folder. Finally a function attached the output files to a SOAP message to

be returned to the client. To make use of the storage space, all files are deleted after returning it to the client. Fig. 11. Shows the overall functionality of the system.

Transferring data is an essential process in CTWS system. Data were transferred through SOAP messages. An XML parser was used to extract data from received SOAP messages either on client or on the server side. Since XML is text-based, transferring binary data (i.e., images, sound etc.) may cause the parser to crash. Several methods were developed to transfer binary data. Transferring data by value (i.e. as embedded content through XML), in Base64 encoding or in hexadecimal text have the disadvantages of increasing encoded data by factor of 1.33X, and 2X respectively for UTF-8 underlying text encoding. Those factors are doubled if UTF-16 text encoding is used. Sending binary data by reference (i.e. attaching binary data as externally unparsed general entities outside of the XML document and then embedding reference URI's to those entities as elements or attribute values) through SWA also have the disadvantage of its heavy reliance on DTD's.

The most powerful method for transferring large amount of data is sending it by reference using AXIOM model and MTOM mechanism. This was the most fit for CTWS system because of the need for transferring large files.

Axis2 as library and tools has been used in encoding CTWS web service. Axis2 contains all the requested classes that simplify and offers extended capabilities for building such services.

## CONCLUSIONS

Throughout the work some points were concluded like Eclipse Ide provides a convenient environment for users to build distributed systems. Axis2 tool save programmer time by providing useful, and easy to use classes for building distributed systems, and a comprehensive methods for exchanging large amount of data between client and servers securely and in a small-size encoding. Also Rock cluster tool is easy to install, easy to use for clustering. Since the interaction among machines; on distributed level, or on cluster machines level is an important aspect of such systems and since the communication time between client and server cannot be accurately calculated, so the statistic methods are the optimal for time analysis for these systems. Despite the fact of what the applications and utilities above provide, there are still problems that relates to compatibility exist



among different software components, and between software and hardware components.

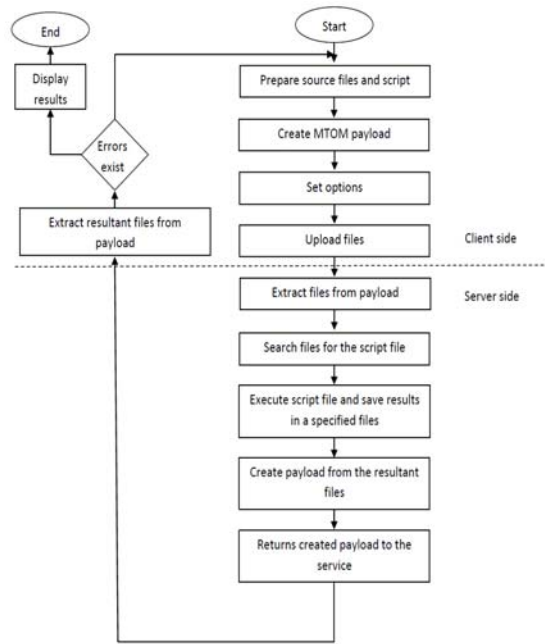


Figure 11. Overall functionality of the system.

## REFERENCES

- [1] Tanenbaum, A. S. and van Steen M., 2002, "Distributed systems Principles and paradigms", Prentice Hall.
- [2] Buyya, R., 1999, "High Performance Cluster Computing Architectures and Systems", Prentice Hall.
- [3] Pfister, G., 1998, "In Search of Clusters", 2nd Edition, 1998, Prentice Hall PTR.
- [4] Harter D. and Zhang L., 2010, "Computational Scientists"
- [5] David, E. C. and Pal, S. J., 1999, "Parallel Computer Architecture: A Hardware/Software Approach", Gulf Professional Publishing.
- [6] Kshemkalyani, A. D. and Singhal, M., 2008, "Distributed Computing: Principles, Algorithms, and Systems", Cambridge University Press, Apr.
- [7] Hwang, K. and Xu, Z., 1998, "Scalable Parallel Computing: Technology, Architecture, Programming", WCB/McGraw-Hill, NY.
- [8] Zahda, S., "Tutorial about Cluster".
- [9] Kehagias, D., Grivas, M., Meletioui, G., Pantziou, G., Sakellarios, B., Sterpis, D., and Ximerakis, D., 2003, "Building a Low-Cost High-Performance Dynamic Clustering System".
- [10] <http://www.sun.com/blueprints>
- [11] Apon A, Buyya R, Jin H, and Mache J, 2001, "Cluster Computing in the Classroom: Topics, Guidelines, and Experiences"
- [12] Lindh, B., 2002, "Sun™ Based Beowulf Cluster", Sun Microsystems AB, Sweden. Available at: [fineit.net/doc/blueprints/1201/beowulf-clstr.pdf](http://fineit.net/doc/blueprints/1201/beowulf-clstr.pdf)
- [13] Harbaugh, L. G., "High-Performance Computing", available at [www.appro.com/uploads/documents/whitepaper.pdf](http://www.appro.com/uploads/documents/whitepaper.pdf)
- [14] Linux web site
- [15] "How to Build a Beowulf Linux Cluster, The Mississippi Center for Supercomputing", [www.mcsr.olemiss.edu/bookshelf/.../how\\_to\\_build\\_a\\_cluster.html](http://www.mcsr.olemiss.edu/bookshelf/.../how_to_build_a_cluster.html)
- [16] Shainer G., Liu T., Layton J., Joshua Mora J., 2009, "Scheduling Strategies for HPC as a Service (HPCaaS)" IEEE.
- [17] Yeo C., et al., 2003, "Cluster Computing: High-Performance, High-Availability, and High-Throughput Processing on a Network of Computers"
- [18] Butler, R., William Gropp, Ewing L, Lusk, 2002, "A Scalable Process-Management Environment for Parallel Programs", 2002, Proceedings of the 7th European PVM/MPI Users' Group Meeting on Recent Advances in Parallel Virtual Machine and Message Passing Interface pp.168 - 175, Springer-Verlag London, UK.
- [19] Boukerche A., Al-Shaikh R., and Notare M., "Towards Building a Highly-Available Cluster Based Model for High Performance Computing"
- [20] Yang C., Liao C., "On Construction and Performance Evaluation of Multiple Linux PC Clusters Using NAT Mechanism",
- [21] Khosrow-Pour, M., 2006, "Emerging Trends and Challenges in Information Technology", Volume 1, Idea Group Inc.
- [22] [english.turkcebilgi.com/Beowulf](http://english.turkcebilgi.com/Beowulf)
- [23] Sterling, T., 2001, "Beowulf Cluster Computing with Windows", MIT Press, Oct.
- [24] Sterling, T., Becker, D., Savarese, D., et al., 1995, "BEOWULF A Parallel Workstation for Scientific Computation", Proceedings of the 1995 Int. Conf on Parallel Processing (ICPP), Vol.1, pp 11-14, August 1995.
- [25] D. Kehagias, M. Grivas, G. Meletioui, G. Pantziou, B. Sakellarios, D. Sterpis, and D. Ximerakis, "Building a Low-Cost High-Performance Dynamic Clustering System".
- [26] Butler, R., William Gropp, Ewing L, Lusk, "A Scalable Process-Management Environment for Parallel Programs", 2002, Proceedings of the 7th European PVM/MPI Users' Group Meeting on Recent Advances in Parallel Virtual Machine and Message Passing Interface pp.168 - 175, Springer-Verlag London, UK 2002.
- [27] [www.rockclusters.org/](http://www.rockclusters.org/)
- [28] Wu, H., Chi, X., and Xu, F., 2002, "Creation of Web-Based User Interface for Supercomputing Environment", Proceedings of the Fifth International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP.02), IEEE.
- [29] Shainer, G., and Liu T., Jeffrey Layton, Joshua Mora, "Scheduling Strategies for HPC as a Service (HPCaaS)"
- [30] Holmes, V. P., Johnson, W. R., Miller, D. J., 2003, "Integrating Web Service and Grid Enabling Technologies to Provide Desktop Access to High-Performance Cluster-Based Components for Large-Scale Data Services", Proceedings of the 36th Annual simulation Symposium (ANSS'03) IEEE.
- [31] Benkner, S., Brandic, I., Engelbrecht, G., Schmidt, R., 2005, "VGE - A Service-Oriented Grid Environment for On-Demand Supercomputing", Proceedings of the 5th IEEE/ACM International Workshop on Grid Computing (GRID'04) 2005 IEEE.
- [32] Peng, L. et al., 2005, "YellowRiver: A Flexible High Performance Cluster Computing Service for Grid", Proceedings of the 8th International Conference on High-Performance Computing in Asia-Pacific Region (HPCASIA'05) 0-7695-2486-9/05 IEEE

## AUTHORS PROFILE

**Dhuha Albazaz** is the head of Computer Sciences Department, College of Computers and Mathematics, University of Mosul. She received her PhD degree in computer sciences in 2004 in the speciality of computer architecture and operating system. She supervised many Master degree students in operating system, computer architecture, dataflow machines, mobile computing, real time, and distributed databases. She has three PhD students in FPGA field, distributed real time systems, and Linux clustering. She also leads and teaches modules at both BSc, MSc, and PhD levels in computer science. Also, she teaches many subjects for PhD and master students.

**Abdulnaser Younis** is a Phd. student in Computer Sciences Department, College of Computers and Mathematics, University of Mosul. He interest with Distributed systems, Databases, and operating system subjects.

# An Optimized Perona-Malik Anisotropic Diffusion Function for Denoising Medical Image

**A.S.M. Delowar Hossain**

Assistant Professor, Dept. of CSE,  
Mawlana Bhashani Science and Technology University  
MBSTU, Santosh, Tangail-1902 (Bangladesh)

**Mehedi Hassan Talukder**

Lecturer, Dept. of CSE,  
Mawlana Bhashani Science and Technology University  
MBSTU, Santosh, Tangail-1902 (Bangladesh)

**Md. Aminul Islam**

Dept. of CSE,  
Mawlana Bhashani Science and Technology University  
MBSTU, Santosh, Tangail-1902 (Bangladesh)

**Md. Azmal Absar Dalim**

Dept. of CSE,  
Mawlana Bhashani Science and Technology University  
MBSTU, Santosh, Tangail-1902 (Bangladesh)

**Abstract**—Noise is the major problem in the field of image processing. In Medical image such as Ultrasound image, MRI data and Radar Images are affected by different types of noise. So it is the most important task to eliminate such noises. In image processing anisotropic diffusion is a technique for reducing image noise without removing significant parts of the image contents, such as edges, lines or other details that are important to represent the quality of the image. To acquire a better performance we state an another diffusion function that works efficiently to denoise an image without blurring the frontiers between different regions. To evaluate the performance we calculate the Signal to Noise Ratio, The Peak Signal to Noise Ratio, The Root Mean Square Error, The Edge Preservative Factor. This Function gives the better result with comparison to existing Perona-Malik anisotropic diffusion Function.

**Keywords**- Anisotropic Diffusion, MRI data, Ultrasound Image, Speckle Noise, Gradient, Performance Evaluation.

## I. INTRODUCTION

Images are often affected by different types of noise such as Salt & pepper noise, Gaussian noise, Speckle noise and mixed noise ( Impulse and Gaussian ) during the transmission, faulty memory location, coherence of waves or timing error. Additive noise is systematic in nature and can be easily modeled and hence removed or reduced easily [1]. Whereas in medical image a multiplicative noise is image dependent complex to model and hence difficult to reduce [1]. The medical image such as ultrasound image is corrupted by speckle noise. Speckle [2] is not a noise in an image but noise-like variation in contrast. Speckle is basically a form of multiplicative noise. Which makes the grayscale of pixels change violently, hides the subtle details and makes the imaging resolution descend greatly. Ultrasound image have a high noise content and suffer poor

contrast. If the MRI image corrupted by noise then an efficient diffusion is required to localize the desired object. In those case the diffusion is most important. So we should use an optimized diffusion function to diffused an image very efficiently. For medical image we often faced Low Signal to Noise Ratio (SNR), Low Peak Signal to Noise Ratio (PSNR), High Root Mean Square Error (RMSE) and Low Edge Preservative Factor (EPF). But if the SNR is too small or the contrast too low it becomes very difficult to detect anatomical structures because tissue characterization fails [3]. For a visual analysis of medical images, the clarity of details and the object visibility are important, so high SNR, PSNR & EPF are required because most of the image segmentation algorithms are very sensitive to noise. In this paper we state an optimized diffusion function to diffused image properly that satisfies the image quality criteria. It diffused an image with improve the SNR, PSNR, EPF and also other image quality measurement parameter.

## II. THE PERONA-MALIK MODEL

Perona and Malik proposed a nonlinear diffusion method for avoiding the blurring and localization problems of linear diffusion filtering. They applied an inhomogeneous process that reduces the diffusivity at those locations which have a larger likelihood to be edges. This likelihood is measured by  $|\Delta I(x,y,t)|$ . The Perona-Malik filter is based on the equation [3]

$$\frac{\partial}{\partial t} I(x,y,t) = \text{div}(G(|\Delta I(x,y,t)|) \cdot \Delta I(x,y,t))$$

$$I(x,y,0) = I_0(x,y)$$

Where,  $\Delta$  is the gradient operator, **div** is the divergence operator,  $||$  denotes the magnitude,  $g(x)$  the diffusion function, and  $I_0$  is the original Image. The intensity change in one iteration step is defined as the sum of the flow contributions between neighboring pixel intensities [3]. The structure is simulated as a network, wherein the center points of pixels represent nodes and are linked together by arcs, whose flow characteristics are determined by the conductivity function Figure 1.

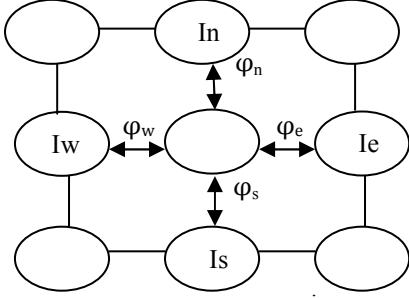


Figure 1: 2D Network Structure

So, the Perona-Malik filtering for 2D image is based on the four nears neighbors by 2D derivation on each pixel of an image.

$$I(x, y, t + \Delta x) \cong I(x, y, t) + \Delta t. (\varphi_{est} - \varphi_{west} + \varphi_{nort} - \varphi_{south})$$

They suggests two diffusion functions

01.  $G1(x) = \exp \left[ - \left( \frac{x}{K} \right)^2 \right]$

02.  $G2(x) = \frac{1}{1 + \left( \frac{x}{K} \right)^2}$

Where K is gradient magnitude and it's value need to be greater than 0.

Other diffusion functions also used to diffused an image [4]. These are given bellow :

03.  $G3(x) = \exp \left[ - \left( \frac{x}{K\sqrt{2}} \right)^2 \right], \quad x \leq K\sqrt{2}$

04.  $G4(x) = 0.5 \left[ 1 - \left( \frac{x}{K\sqrt{2}} \right)^2 \right], \quad x \leq K\sqrt{2}$

05.  $G5(x) = 0.67 \left[ 1 - \left( \frac{x}{K\sqrt{5}} \right)^2 \right], \quad x \leq K\sqrt{5}$

### III. PROPOSED DIFFUSION FUNCTION

Our proposed diffusion function is given by the following equation :

$$G6(x) = 0.5 \left[ 1 - \left( \frac{x\sqrt{3}}{K\sqrt{2}} \right)^2 \right], \quad x \leq K\sqrt{2}$$

Where K is gradient magnitude and it's value need to be greater than 0.

### IV. EVALUATION CRITERIA

To validate the efficiency of this model we have defined some statistical criteria of image performance. Additionally to subjective visual evaluation, it is desirable to present quantitative measure. The parameters which are used in estimation of performance are SNR, PSNR, RMSE, EPF, RMSE\_SNR, IFy, MSSIM.

#### A. Signal to Noise Ratio (SNR) :

The Signal to Noise Ratio SNR is estimated by the following formula [5] :

$$SNR = \left[ \frac{\sum_{x=1}^M \sum_{y=1}^N f2(x,y)^2}{\sum_{x=1}^M \sum_{y=1}^N (f2(x,y) - f1(x,y))^2} \right]$$

Where f1 means original Image and f2 means diffused Image. M×N is size of Image and x means row and y means columns.

#### B. Peak Signal to Noise Ratio (PSNR) :

The Peak Signal to noise Ratio PSNR is estimated be the following formula [5]:

$$PSNR = 10 \log \left[ \frac{255^2}{MSE} \right]$$

Where,  $MSE = \left[ \frac{\sum_{x=1}^M \sum_{y=1}^N (f1(x,y) - f2(x,y))^2}{M*N} \right]$

Where f1 means original Image and f2 means diffused Image. M×N is size of Image and x means row and y means columns.

#### C. Edge Preservative Factor (EPF) :

The Edge Preservative Factor [5] can be computed by the following equation:

$$EPF = \frac{\Gamma(f1 - \bar{f1}, f2 - \bar{f2})}{\sqrt{\Gamma(f1 - \bar{f1}, f2 - \bar{f1}). \Gamma(f2 - \bar{f2}, f2 - \bar{f2})}}$$

Where,  $\Gamma(s1, s2) = \sum_{i=1}^k s1.s2$

Where f1 means original Image, f2 means diffused Image and  $\bar{f}_1$  &  $\bar{f}_2$  represents the Mean of Original image and diffused

image respectively. K is size of Image and x means row and y means columns.

#### D. Root Mean Square Error (RMSE) :

The Root Mean Square Error RMSE [5] calculated by the following equation:

$$RMSE = \sqrt{MSE}$$

#### E. Root Mean Square of Signal to Noise Ratio (RMS\_SNR) :

The Root Mean Square of Signal to Noise Ratio RMS\_SNR [6] calculated by the following equation:

$$RMS\_SNR = \sqrt{\frac{\sum_{x=1}^M \sum_{y=1}^N f_2(x,y)^2}{\sum_{x=1}^M \sum_{y=1}^N (f_2(x,y) - f_1(x,y))^2}}$$

Where f1 means original Image and f2 means diffused Image. M×N is size of Image and x means row and y means columns.

#### F. Image Fidelity (IFy) :

The Image Fidelity [7] is defined by :

$$IFy = 1 - \frac{1}{SNR}$$

#### G. Measuring Similarity between two image (MSSIM) :

MSSIM is used for measuring the similarity between two images i.e. similarity between original image and diffused image. Higher the MSSIM between original and filtered image gives lower the noise in filtered image [8]. MSSIM [9] is given by

$$MSSIM(x, y) = \frac{1}{M} \sum_{j=1}^M SSIM(x_j, y_j)$$

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

Where,

$$\mu_x = \frac{\sum_{i=1}^N w_i x_i}{\sum_{i=1}^N w_i}$$

$$\sigma_x = \sqrt{\sum_{i=1}^N w_i (x_i - \mu_x)^2}$$

$$\sigma_{xy} = \sum_{i=1}^N w_i (x_i - \mu_x) (y_i - \mu_y)$$

$$c_1 = (K_1 L)^2$$

$$c_2 = (K_2 L)^2$$

And

Where, L is the range of pixel values (255 for 8-bit grayscale images). And  $K_1 \ll 1$  is a small constant and also  $K_2 \ll 1$ .

## V. EXPERIMENTAL RESULTS

To validate the efficiency of our proposed method, the simulation study has been carried out using MATLAB image processing Toolbox. Two standard Medical image one is MRI image and other is Ultrasound image are selected for simulation study. Firstly we select the Contaminated MRI image and diffused it by the nonlinear Perona-Malik method [3] using the existing diffusion function and also diffused it by using our proposed function. Secondly we select an ultrasound image with multiplicative noise and diffused it. For those two image our proposed method is compared with existing method which are shown in Table 1 and Table 2 respectively.

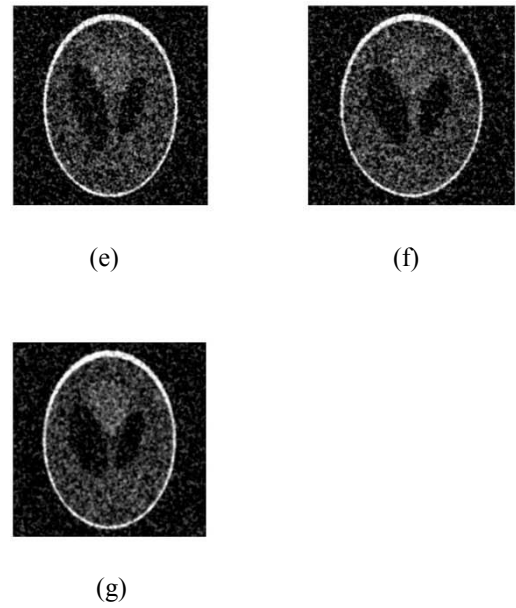
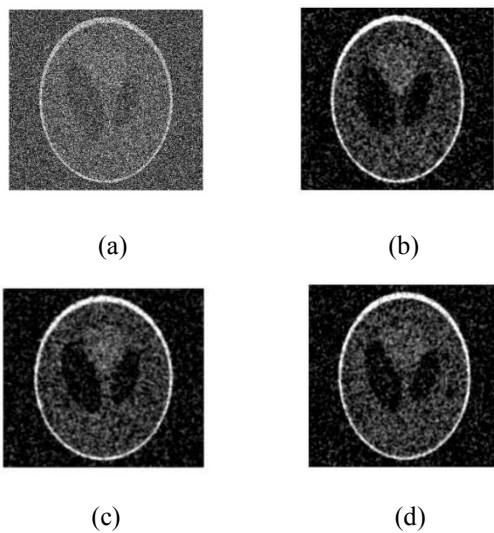
**Table 1:** Comparison of Existing Perona-Malik Diffusion Functions and Proposed Function for MRI Image

Criteria	Diffusion function G1	Diffusion function G2	Diffusion function G3	Diffusion function G4	Diffusion function G5	Proposed Diffusion function G6
SNR	0.0661	0.0645	0.0677	0.0886	0.0766	0.0904
PSNR	48.2776	48.2599	48.2865	48.4695	48.3796	48.5228
RMSE	0.9843	0.9853	0.9822	0.9572	0.9718	0.9559
EPF	0.0709	0.0703	0.0709	0.1472	0.1000	0.1484
RMS_SNR	0.2571	0.2540	0.2603	0.2878	0.2765	0.3006
IFy	-14.1287	-14.4995	-13.7632	-10.2828	-12.0593	-10.0669
MSSIM	0.9915	0.9914	0.9914	0.9979	0.9976	0.9989

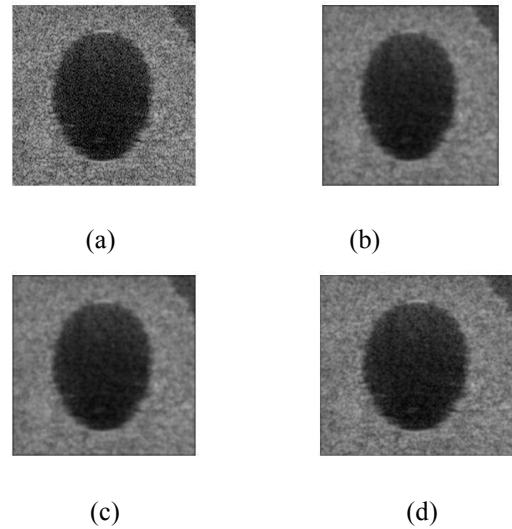
**Table 2:** Comparison of existing Perona-Malik Diffusion Functions and Proposed Function for Ultrasound Image

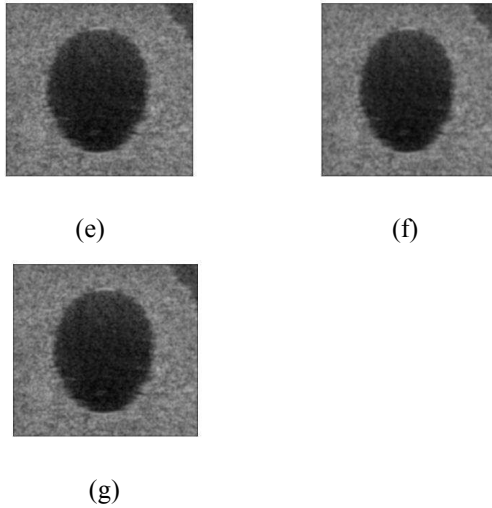
Criteria	Diffusion function G1	Diffusion function G2	Diffusion function G3	Diffusion function G4	Diffusion function G5	Proposed Diffusion function G6
SNR	40.1473	40.1473	40.1464	76.2042	56.2445	76.2151
PSNR	72.2660	72.2660	72.2659	74.9795	73.6884	74.9801
RMSE	0.0621	0.0621	0.0621	0.0455	0.0527	0.0455
EPF	0.7411	0.7411	0.7411	0.8416	0.7950	0.8418
RMS_SNR	6.3362	6.3362	6.3361	8.7295	7.4996	8.7301
IFy	0.9751	0.9751	0.9751	0.9865	0.9822	0.9869
MSSIM	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

Visual Comparison are shown in Figure 2 and Figure 3.



**Figure 2.** a). Original Noisy MRI Image, b). Diffused Image using G1, c) Diffused Image using G2 d). Diffused Image using G3, e). Diffused Image using G4, f). Diffused Image using G1, g). Diffused Image using Proposed Diffusion function.





**Figure 3.** a). Original Noisy Ultrasound Image, b). Diffused Image using G1, c) Diffused Image using G2, d). Diffused Image using G3, e). Diffused Image using G4, f). Diffused Image using G1, g) Diffused Image using Proposed Diffusion function.

## VI. CONCLUSION

Image denoising has become a crucial step for correct diagnosis. The current need of healthcare industries is to preserve useful diagnostic information with minimum noise. In this paper, the proposed diffusion function's performance for denoising an image is evaluated both subjectively and objectively. The experimental results prove that the proposed model produces images which are cleaner and smoother and at the same time kept significant details, resulting in a clearer and appealing vision. The experimental result also shows that the proposed function restores the fine details, such as lines, frontiers and corners efficiently and shows better results when comparing with other standard diffusion function.

## VII. REFERENCES

- [1] "IMAGE INDEPENDENT FILTER FOR REMOVAL OF SPECKLE NOISE". IJCSI INTERNATIONAL JOURNAL OF COMPUTER SCIENCE ISSUES, VOL. 8, ISSUE 5, NO 3, SEPTEMBER 2011.
- [2] J. W. Goodman, "Some fundamental properties of speckle," *J. Opt. Soc. Amer.*, vol. 66, no. 11, pp. 1145–1149, 1976.
- [3] "Nonlinear Anisotropic filtering of MRI data". IEEE TRANSACTIONS ON MEDICAL IMAGING. VOL. 11. NO. 2. JUNE 1992 :
- [4] "On the choice of the parameters for anisotropic diffusion in image processing".
- [5] "Digital Image Processing". Third Edition By Rafael C. Gonzalez .
- [6] "Filtering Corrupted Image and Edge Detection in Restored Grayscale Image Using Derivative Filters". International Journal of Image Processing, (IJIP) Volume (3) : Issue (3).
- [7] [www.google.com](http://www.google.com)
- [8] Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, "Image quality assessment: From error measurement to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
- [9] "Image Independent Filter for Removal of Speckle Noise". IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011.

# New Paradigm for MANET Routing using Right Angled Biased Geographical Routing Technique (RABGR)

**Mr. V J Chakravarthy**

*Research Scholar*

*P.G. Research Dept of Com. Science*

*D G Vaishnav College, Arumbakkam, Chennai 600 106.*

**Capt. Dr. S Santhosh Baboo**

*Associate Professor*

*P.G. Research Dept of Com. Science*

*D G Vaishnav College, Arumbakkam, Chennai 600 106.*

**Abstract—** In this paper, we analyze the benefits of optimal multipath routing, to improve fairness and increase throughput in wireless networks with location information, in a bandwidth limited ad hoc network. In such environments the actions of each node can potentially impact the overall network connections. This is done by making multipath routing method, named as Right Angled Biased Geographical Routing (RABGR), and two congestion control algorithms, Biased Node Packet Scatter (BNPS) and Node-to-Node Packet Scatter (NNPS), which enhances the RABGR to avoid the congested areas of the network. The above RABGR method is used with AODV and AOMDV protocols and their results are compared. After Simulation, the experimental results shows that the solution achieve its objectives. Extensive ns-2 simulations show that the solution improves both fairness and throughput as compared to greedy routing using only single path.

**Keywords-** MANET, AODV, AOMDV, Biased geographical routing, congestion, greeding routing.

## I. INTRODUCTION

In ad hoc networks, nodes self-organize to create a mesh, in which each node can act as of a source, a destination or a relay for traffic. The flexibility offered in such networks may be tackled in variety of contexts. For example, In disaster areas or in search-and-rescue operations, it is very appealing to be able rapidly deploy a wireless ad hoc networks without the need of a fixed infrastructure. However, because of adverse channel conditions and potential node mobility, traditional networking tasks such as routing can be challenging even when the number of nodes is limited. Several distributed routing protocols exist and have been tailored to wireless ad hoc networks. Routes can either be stored in routing tables and periodically updated at each node, or discovered on demand by the sources. In most wireless ad hoc networks, the action of a single user may affect the rest of the network, for instance by saturating a bottleneck link. Consequently, the network conditions may change frequently. This makes traditional table driven algorithms less efficient and motivates the use of on-demand source routing

protocols. Some of these types extend to multipath routing and provide several mostly independent path. The use of multiple routes reduces the frequency of path updates and increases robustness against changes in the network algorithm.

Wireless embedded processors contained in mobile phones, handled devices or weaved into the environment as sensors, are likely to become the main part of the future Internet. So, geographical routing, an algorithm using greedy manner leverages location information to route messages in multipath routing techniques.

In this paper, we present a high efficient solution that seeks to utilize idle or under-loaded nodes to reduce the effects of congestion. To work out this, we highly enhanced the geographical routing to allow a source to select different paths to make the packet to reach the destination. First, we propose multi-path solutions for geographic routing which has less effective results, at the end, we likely to propose right angled biased geographical routing technique (RABGR), a lightweight, stateless, Geographical forwarding algorithm, as cost effective complement to greedy routing. The above RABGR routes packets in straight path i.e. 90° from the source, instead the shortest path, towards the destination.

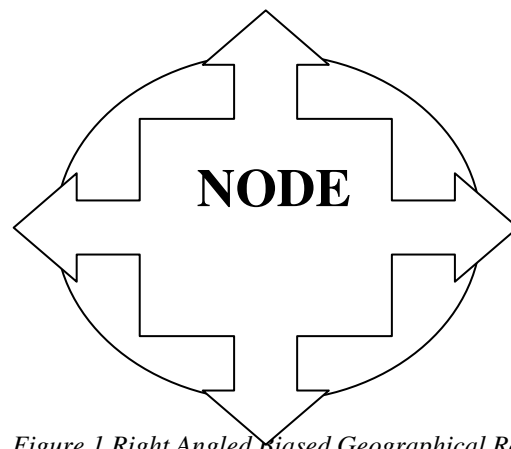


Figure 1. Right Angled Biased Geographical Routing

The reduce the congestion during transmission of packets; we propose two more congestion control mechanisms that highly enhance RABGR.

#### A. Biased Node Packet Scatter (BNPS)

**BNPS** is a very light weight method mechanism that partially aims to transient congestion by locally splitting the traffic along multiple paths to avoid congested hotspots. BNPS splits flows close to the congestion point. Each node monitors the congested status of all its neighbours and splits the flows that are going towards a congested neighbour, if the node itself is congestion. The scattered packets contain bias of  $90^\circ$ , such that the modified paths quickly move away from the original path.

#### B. Node-to-Node Packet Scatter (NNPS)

**NNPS** is also a mechanism but aim to transmit packets to longer term congestion, when BNPS fails. If BPNS cannot successfully support the aggregate traffic, it will only scatter packets to a wider area potentially amplifying the effects of congestion collapse due to its longer paths.

The performance of the above two mechanism had been evaluated in term RABGR by using a high-level simulator, a packet-level simulator (NS-2). The results show that RABGR is a practical and efficient multipath routing algorithm. We have evaluated BNPS and NNPS using NS2.

#### C. AODV - The Ad Hoc On-demand Distance-Vector Protocol

Ad Hoc On-demand Distance-Vector (AODV) Protocol is a routing algorithm used in ad hoc networks. In AODV, each node maintains a routing table which is used to store destination and next hop IP addresses as well as destination sequence numbers. Each entry in the routing table has a destination address, next hop, precursor nodes list, lifetime, and distance to destination.

#### D. AOMDV - The Ad Hoc On-demand Multipath Distance-Vector Protocol

Ad-hoc On-demand Multi path Distance Vector (AOMDV) protocol is an extension to the AODV protocol for computing multiple loop-free and link disjoint paths. The routing entries for each destination contain a list of the next-hops along with the corresponding hop counts. All the next hops have the same sequence number. This helps in keeping track of a route. For each destination, a node maintains the advertised hop count, which is defined as the maximum hop count for all the paths, which is used for sending route advertisements of the destination.

### II. THE RIGHT ANGLED BIASED GEOGRAPHICAL ROUTING (RABGR)

The requirements of the RABGR algorithm are as follows. In addition, we present simulation results that show that BGR achieves good performance with a low overhead.

#### A. Design goals

Wireless network with coordinate based routing. To have sensor networks, we require stringent energy and computational constraints, which characterize these networks.

#### B. The requirements of the geographic routing protocol

- **Low communication overhead** – packets sent by the sensor nodes are very small e.g. the maximum packet size is 29 bytes.
- **Simplicity** – The routing algorithm must have low computational overhead e.g. 4 kB of RAM.
- **Low state** – nodes much maintains a minimal amount of state i.e. no per-flow or per-path state in network. In addition, to avoid the hotspots in the considered wireless networks, a multi-path algorithm should be there, that must be able to provide a large number of path i.e.,  $90^\circ$ , with few common hops without increasing routing failures, as compared to the single-path greedy routing.

### III. EXPLANATION OF THE RIGHT ANGLED BIASED GEOGRAPHICAL ROUTING (RABGR)

The main idea in our solution is to reduce the congestion during the transmission of packets form source to destination, is to insert a "**BIAS**" i.e. the angle in each packet, which determines the straight line path from the source so that the packets move towards the destination. Here the term bias is a measure angle of which the packets take from the source from greedy route and also indicates the side of deviation. In our discussion, the term bias is treated at each hop as an angle i.e.,  $90^\circ$ . Instead of routing greedily towards the destination. RABGR routes greedily towards the point P2 (target point) situated at a predefined distance from the current node point P1 such that the angle between the lines P1P2 and P1D is equal to the bias i.e angle  $90^\circ$ .

In wireless networks, Congestion occurs when the wireless area around them is busy. With networks congestion is mostly situated at the border of the network, with point to point communication congestion usually builds in the center. So avoid the congestion in the wireless networks, the way should be followed, i.e., we allow packets to route on alternate paths. This type of routing avoid the congestion is busy area in the wireless networks.

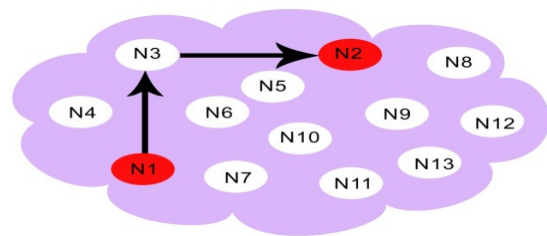


Figure 2. RABGR Packet Forwarding using Right angle Method - minimising Congestion in Wireless Networks.

#### A. BNPS – Biased Node Packet Scatter

BNPS splits flows close to the congestion point. Each node monitors the congested status of all its neighbours and splits the flows that are going towards a congested neighbour, if the node itself is congestion. The scattered packets contain bias of  $90^\circ$ , such that the modified paths quickly move away from the original path.



### B. NNPS – Node – to – Node Packet Scatter

If BPNS cannot successfully support the aggregate traffic, it will only scatter packets to a wider area potentially amplifying the effects of congestion collapse due to its longer paths.

### C. Evaluation of BNPS and NNPS

In this section we present simulation results obtained through NS-2 simulations. We use three main metrics for our measurements: throughput increase, packet delivery ratio and delay among flow.

We ran tests on a network of 20 nodes, distributed uniformly on a grid in a square area of 1000m x 1000m. We assume events occur uniformly at random in a geographical area; the node closest to the event triggers a communication burst to a uniformly selected destination. To emulate this model we select a one set of random source-destination pair and run 20 second synchronous communications among the selected pair. The data we present is averaged over hundreds of such iterations. The parameters are summarized in Table 1.

TABLE I. SUMMARY OF PARAMETERS

Parameter	Value	Parameter	Value
Number of Nodes	50	Link Layer Transmission Rate	2 Mbps
Area Size	1000m x 1000m	RTS / CTS	No
MAC	802.11	Retransmission Count (ARQ)	No
Radio Range	100m	Interface Queue	No
Contention Range	250 m	Packet Size	100B
Average Node Degree	90	Packet Frequency	50/s

### IV. PERFORMANCE METRICS

We used out RABGR for AODV protocol with the AOMDV protocol. We evaluate mainly the performance according to the following metrics, by varying the pause time as 0, 1, 2, 3, 4, 5, etc....

#### A. Throughput:

It is the number of packets received successfully. In communication networks, such as Ethernet or packet radio, throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

#### B. Average Packet Delivery Ratio:

It is the ratio of the number of packets received successfully and the total number of packets sent.

#### C. Average end-to-end delay:

The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

### V. SIMULATION RESULTS

#### A. Based on Pause time

In our initial experiment, we vary the pause time as 0, 1, 2, 3, 4, 5, etc....

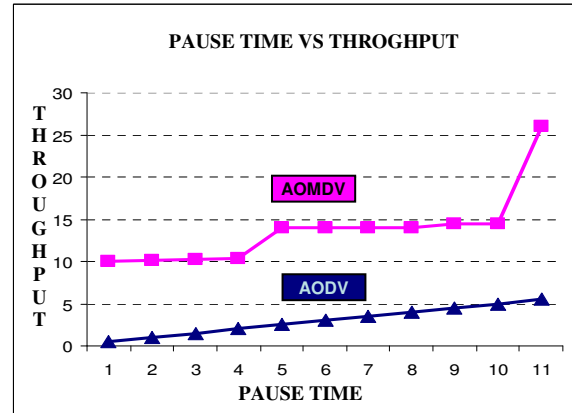


Figure 3. Pause time Vs Throughput

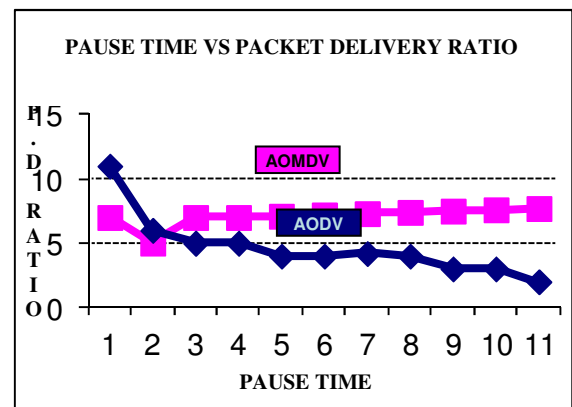


Figure 4. Pause time Vs Packet Delivery Ratio

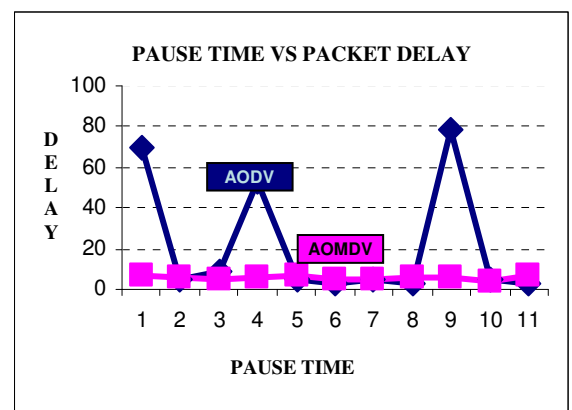


Figure 5. Pause time Vs Packet Delay

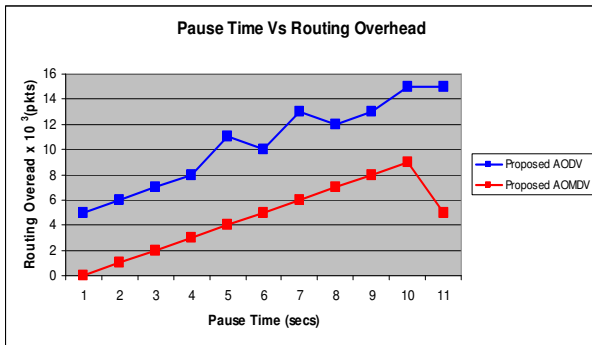


Figure 6. Pause time Vs Routing Overhead

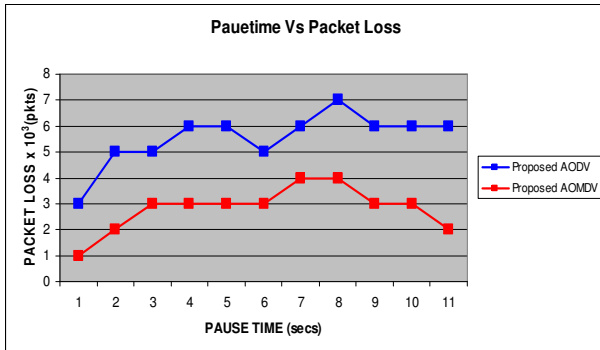


Figure 7. Pause time Vs Packet loss

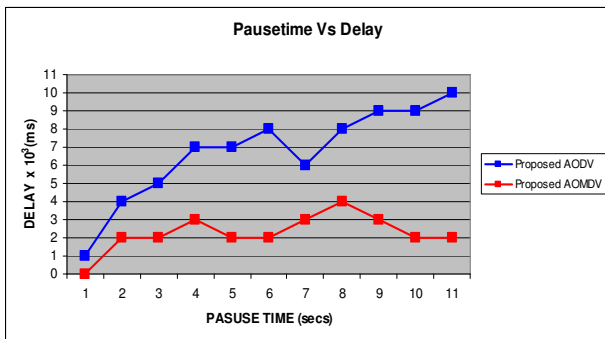


Figure 7. Pause time Vs Delay

From Figure 2, 3, 4, 5, 6 and 7 clearly proves that working of RABGR with AOMDV protocol gives the increased Throughput, increased Packet Delivery Ratio and decreased Packet Delay.

## VI. CONCLUSION

In this paper, initially we have presented a solution for one source and one destination that increases fairness and throughput at the same time decreases the packet loss in dense wireless networks. Our overall experiment achieves its goal by using multipath geographic routing to find resources in the wireless network by AOMDV when compared with AODV protocol. The algorithm we used is simple and has low communication overhead; simulation results we got also show favourable results, showing that the RABGR works well with AOMDV protocol. The proposed two algorithms i.e., BNPS

and NNPS that made a flow through 90° in the multiple paths when it is experiencing congestion. In this practice we also combine both BNPS and NNPS to have more enhanced result. By simulation results, we have proved that our proposed routing method attains high throughput and packet delivery ratio, by reducing the packet delay. In the future work, we plan to propose a new protocol using RABGR method with security

## REFERENCES

- [1] Pister K. S. J. Kahn J. M. And Boser B. E. "Smart Dust: Wireless Networks of Millimeter – Scale. Sensor Nodes." in Electronics Research Laboratory Research Summary, 1999.
- [2] Roa A. Ratnsamy S., Papadimitriou C., Shenkder S., Stoica I., "Geographic Routing without Location Information," in Proc. Of Moicom, 2003.
- [3] "The New Simulator – ns-2" <http://www.isi.edu/nsnam/ns/>.
- [4] Stoica, David S. Rosenblum "Reducing Congestion Effects in Wireless Networks by Multipath Routing
- [5] W. Heinzelman, A. Chandrasanan, H. Balakrishnan: Energy-efficient communication protocol for wireless sensor networks, in: Proceeding of the Hawii International Conference System Sciences, Hawii (January 2000).
- [6] Seungjoon Lee, Bobby Bhattacharjee "Efficient Geographic Routing in Multihop Wireless Networks".
- [7] Moore D. Leonard J Rus d. and Teller s., "Robust Distributed Network Localization with Noisy Range Measurements", in Proc of Sensys 2004.
- [8] The Berkely Intel Research Mirage testbed, <http://mirage.berkeley.intel-research.net/>.
- [9] Ramakrishna Gummadi, Ramesh Govindan, Nupur Kothari, Brad Karp, Young-Jin Kim, Scott Shenker, "Reduced State Routing in the Internet", in Proc. Of Hotnets 2004.
- [10] Jinlyang Li, John Lannotti, Douglas S.J. De Couto, David R. Karger.
- [11] Robert Morris – Ad Hoc Routing – in Proc of Mobicom, 2000.
- [12] Peter P. Pham and Sylvie Perreau, "Performance Analysis of Reactive Shortest Path and Multipath Routing Mechanism with Load Balance", in Proc. Of Infocom, 2003.
- [13] Piyush Gupte, P. R. Khumar, "Capacity of Wireless Networks", in IEEE Transactions on Information Theory, 46/2, March 2000.
- [14] Levis P. Lee N., Welsh M., and Culler D., "TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications," in Proc. Of SenSys, 2003.
- [15] A Roa et al., "Geographical routing without location information." in IEEE/ACM MobiCom, Sep. 2003.
- [16] Brad Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks, "in proceedings of the 6th ACM/IEEE MobiCom. 2000, pp. 243-254, ACM Press.

## AUTHORS PROFILE



**Capt. Dr. S .Santhosh Baboo**, aged forty five, has around twenty one years of postgraduate teaching experience in Computer Science, which includes Six years of administrative experience. He is a member, board of studies, in several autonomous colleges, and designs the curriculum of undergraduate and postgraduate programmes. He is a consultant for starting new courses, setting up computer labs, and recruiting lecturers for many colleges. Equipped with a Masters degree in Computer Science and a Doctorate in Computer Science, he is a visiting faculty to IT companies. It is customary to see him at several national/international conferences and training programmes, both as a participant and as a resource person. He has been keenly involved in organizing training programmes for students and faculty members. His good rapport with the IT companies has been instrumental in on/off campus interviews, and has helped the post graduate students to get real time projects. He has also guided many such live projects. Capt..Dr. Santhosh Baboo has

authored a commendable number of research papers in international/national Conference/journals and also guides research scholars in Computer Science. Currently he is Associate Professor in the Postgraduate and Research department of Computer Science at Dwaraka Doss Goverdhan Doss Vaishnav College (accredited at 'A' grade by NAAC), one of the premier institutions in Chennai.



**Mr. V J Chakravarthy**, done his Under-Graduation in Madras University and Post-Graduation in Bharathidasan University and Master of Philosophy Degree in Periyar University. He had published good no of papers in the national / international journal. His work is mostly based on wireless networks – proposing new protocols based on security concepts. He is currently pursuing his Ph.D

# Development of an Intelligent GIS application for spatial Data analysis.

Pro.Dr. Hesham Ahmed Hassan  
Head of Computer Science Department.  
Faculty of Computers and Information.  
Cairo University

Dr. Mohamed Yehia Dahab  
A Central Laboratory of Agriculture  
Expert System.  
Agriculture Research Center

Eng. Hussein Elsayed Elsayed Abla  
B.Sc. Computer Science  
Cairo University, 2005  
Email.cpp\_abla@hotmail.com

## Abstract:

No one can deny Ambulance, Fire engine and police stations role in society service and feel all people safety and assurance, so we aim to get high performance and offer a good service through improve answer rate and Ambulance, Fire engine Centers and police stations distribution. Thus we integrated Geographic Information Systems (GIS) applications with domain expertise are saving time, effort and cost. The system aids the personnel to get critical spatial and non-spatial information. The system can identify the nearest Ambulance or Fire engine or police stations to the emergency location, and also determine the shortest route from the selected Ambulance station to the emergency location This framework is integrated GIS sciences can help users visualize map information and display spatial representations and suggestions for assessing existing Ambulance and Fire engine Centers performance hence planning and simulating for the future to approach for a good prediction and decision making with both static and dynamic spatial data.

**Keywords—** *Development of an Intelligent GIS application for spatial Data analysis; Emergency planning; Shortest route analysis; Decision making;*

## I. INTRODUCTION

An emergency event is uncertain, sudden, and complex for analysis. Emergencies are either caused by a natural disaster or deliberate. Natural disasters include earthquakes, floods, fires, tsunami, tornadoes, hurricanes, volcanic eruptions, or landslides.

In recent years, the world has experienced many crises related to disaster and emergency occurrences. Those crises usually cause a great loss of population and wealth. It has been critical to save as much as lives as possible. In light of the increasing urban communities, and with the rowing possibility of disasters' occurrences, whether natural or deliberate, it has become imperative to establish an effective plan to manage the disaster and try to reduce losses as much as possible [1][2].

A Geographic Information System (GIS) is mapping software that provides spatial and special data by linking locations with information about that location. It provides the functions and tools needed to efficiently capture, store, manipulate, analyze, and visualize information on locations on map [3][4].

GIS is becoming an increasingly important tool in

environmental management, retail, military, tourism, routing, police and many other spheres of our daily lives. GIS are computer-based systems that enable users to collect, store, process, analyze and present spatial data [5]. It provides an electronic representation of information, called spatial data, about the Earth's natural and man-made features.

A Decision Support Systems (DSS) is a computer application system to assist decision makers in solving structured or unstructured problems. It provides an environment for decision makers to analyze problems, build models, simulate processes and programs, and calls information resources or analytical tools for decision makers [1].

Decision Support Systems (DSS) have exploited the GIS ability to use geography and linking location to information, to help make better, more informed decisions and assist decision makers in a wide variety of fields [6]. The need to use spatial data in many of these diverse fields has led to increasing interest in the development of Spatial Decision Support Systems (SDSS) based around GIS technology [7].

GIS uses geography and computer-generated maps as an interface for integrating and accessing

massive amounts of location-based information. GIS software helps co-ordinate vast amounts of location-based data from multiple sources. It enables the user to layer the data and view the data most critical to the particular issue or mission.

The use of DSS would improve the efficiency of evacuation and also reduces life or property loss. The focus in emergency management is to prevent disasters or mitigate them when they occur as fast as possible. Accurate and reliable information and spatial data on disaster and how to quickly deal with the statistical summary and analysis requires efficiency and effectiveness [1].

Ongoing analysis using GIS could have identified safe transport routes to the responding agencies and healthcare personnel. Also, depending on how often data is updated, a GIS could have assisted decision makers in responding to medical supply levels and other variables that change through time.

This framework enables person to plan effectively for emergency response, determine mitigation priorities, analyze historical events, and predict future events. It is used world over by center room department, both large and small, to provide mapping solutions for emergency analysis, traffic safety, community policing, routing and numerous other tasks [8].

This paper is organized as follows, review of previous studies in section (II), description of the methodology of the system in Section (III), Results are presented and discussed in Section (IV), and finally conclusion and future work is presented in section (V).

## II. LITERATURE REVIEW AND RELATED

The study of geographic information systems (GIS) is centered on the designs, processes, and methods that integrate people, spatial data, exploratory tools, and structured discussions for planning, problem solving, and decision-making. Geographic Information Systems is an edited book that integrates relevant theoretical frameworks, methods, and the latest research findings for group planning, problem solving, and decision making using GIS-based technologies. Research into supporting human decision-making processes through the use of computer-based applications is well established in many fields. This research includes the spatial data domain that, although relatively young by comparison, which has produced a large literature. Several threads of research are intertwined within and between specific application areas that use spatial data resources (such as health, education, urban planning, resource management, etc.). These

threads have persisted in the literature and have recently diverged into several new areas.

Various research studies have presented a wide range of Spatial Decision Support Systems (SDSS) applications. These SDSS applications have used various technologies and approaches to address spatial decision making situations from a variety of disciplines or domains.

Such applications can be used in many important areas, such as marketing, land use, disaster management, risk management, routing and crime analysis [8][9][10][11].

Some researches focus on real-time evacuation systems based on GIS [1] [3] [4]. Emergency decision-making system developed in [1] consists of three main components: video surveillance subsystem, network communication subsystem, and information processing and DSS. It adopts development mode on Web GIS platform, using high-level programming language. It incorporates models such as leakage calculation model, leaking hazardous computing model of toxic substances, fires and explosions computing model and the optimal evacuation models.

Blue-Arrow system developed in [2] supports three algorithms: minimum evacuation time algorithm, maximum evacuation capacity algorithm, and the shortest path. AJAX, JavaScript, XML, and CSS are used to build a UI for the client tier, Apache Tomcat is the web server tier, and the ESRI Shapefile is used as the data tier [3].

The architecture designed in [4] integrates computational simulation models based on GIS and databases. Disaster evolution prediction, impact areas demarcation, human behavior simulation and real-time data acquisition were integrated [4]. Evacuating large-scale building or public squares is also studied in [5] [6] [7] [8].

A GIS-based chemical emergency management system is built to help with decisions about the degree of hazard posed by the incident and this information could draw emergency response plans in order to prevent the incident [5]. The system provides two different types of emergency planning: emergency planning of individual installations including public utilities and disaster planning of the government. The system's architecture is based on the integration of IIS web server, Mapserver, and MySQL database. The application consists of a form-based component developed with PHP and a geographical component developed with UMN MapServer.

Other studies focus not only on natural phenomena but also on traffic accidents [12] [13]. In [12] three-tier architecture system is developed. Emergency situation and its relevant basic treatment are shown as a result based on an input of and alarming point on map. In [13] A Highway Emergency Response

System (HERS) is based on a data fusion technology and an intelligent decision support technology. It aims to develop a reliable, easy to use, and scalable platform, which can be used to optimize the layout of the emergency resources and provide an effective and reliable security for rapid response.

Iwanski developed a Criminal Movement Model (CriMM) to investigate the relationship between simulated travel routes of offenders along the physical road network and the actual locations of their crimes in the same geographic space [14]. With knowledge of offenders' home locations and the locations of major attractors, the model was able to determine the routes that offenders are likely to take when travelling from their home to an attractor by employing variations of Dijkstra's shortest path algorithm. The model was run in MatLab 2009a on a Linux operating system. It can be concluded that GIS is widely used in crime analysis. GIS offers many tools for effective Emergency mapping, analysis and management. It has many applications and promotes collaborations across a wide variety of disciplines.

### III. METHODOLOGY

#### *System Architecture*

This section presents an explanation of the system's architecture and an overview of the technologies and tools used to develop the proposed system. Figure 1 shows the main components of the system. The system architecture is a three-tier architecture system: the user tier layer, the GIS engine tier layer, and the data tier layer.

The user layer is the interface between the user and the system. An input form implicitly calls the MapObject® engine components which in turn access the database. The data layer contains the underlying database, including both the spatial database and the attribute database. Based on this architecture, framework provide many roles in spatial Data analysis like information retrieval, thematic mapping, spatial measurement, overlay, buffer and corridors and network analysis which used in case study for assessment, planning, simulation and decision making .

The framework is powerful user interface which enable to select region which we need to assessment it can view region as demography data according the attribute which you select this attribute can be number of ambulance cars, distribution of ambulance center, number of population divided to some category according age stage, social state, education state, gender state and income level,..., etc.

In case ambulance centers we can detect location in map visually and view relations between ambulance centers and all geographic aspects life from

building, and elements of human attracting like (restaurant, entertainment places, commercial center, hospitals, ..., etc) according to number of kilometers or number of population which represent services ranges and answer rate that ambulance can introduce according to some rules the user first marks a new emergency event on a map and an event is instantly added into a new layer associated with a table in the database. The spatial analyst (a GIS engine component) is requested to calculate the buffer zone and the evacuation path with the shortest route to the nearest health care facility is displayed on map.

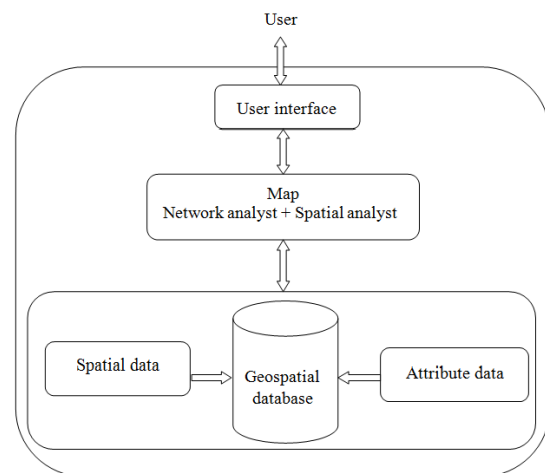


Figure 1. System Architecture

ArcGIS® 9® is an integrated collection of software products for building a complete GIS which was developed by ESRI [15].

The proposed system in this study is developed using MapObject® 2.3. The software package facilitates modeling by providing VB (Visual Basic) which is used to develop this system using component-based geographic data models:

MapObject®. Some capabilities of both spatial analyst [16] and network analyst [17] are incorporated into the system as well.

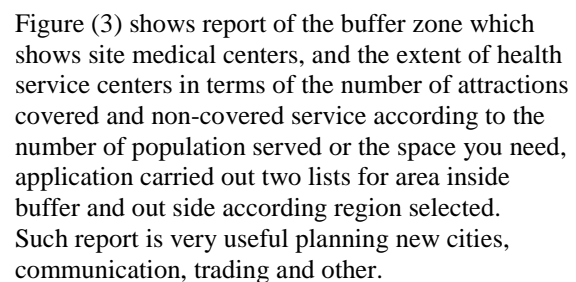
MapObject® services can be categorized as base services, data access, map analysis, map presentation, developer components and Web development framework, and user interface and extensions. MapObject® VB is used to build the user interface for emergency event's data input and MapObject® was also combined with the code to read/write the database (shape files) and to display the buffer and other information over the map. One of the features applied in this system is buffer analysis and overlay which are feature-based user defined. Buffers are usually used to delineate protected zones around features or to show areas of influence. They calculate distances from spatial objects, and produce polygons that reflect the object and the area around it. Buffer zones are frequently used to mitigate environmental hazards [18].



To get the shortest route to the intended location, the user first has to locate both current and intended locations on the map, then the evacuation analysis tool implicitly calls the network analyst extension, and calculates the shortest route, and it is displayed on the map when the user chooses to get the solution.

The Application has a basic function that is to determine the service range for health center to

And also it can view region as demography data according the attribute which you select this attribute can be number of ambulance cars, distribution of ambulance center, number of population as shown In figure (2) which is very useful for assessment Present case and planning for the future which also describes the reasons why GIS is becoming increasingly important, day after day, to help decision-makers to make decisions quickly and wisdom.



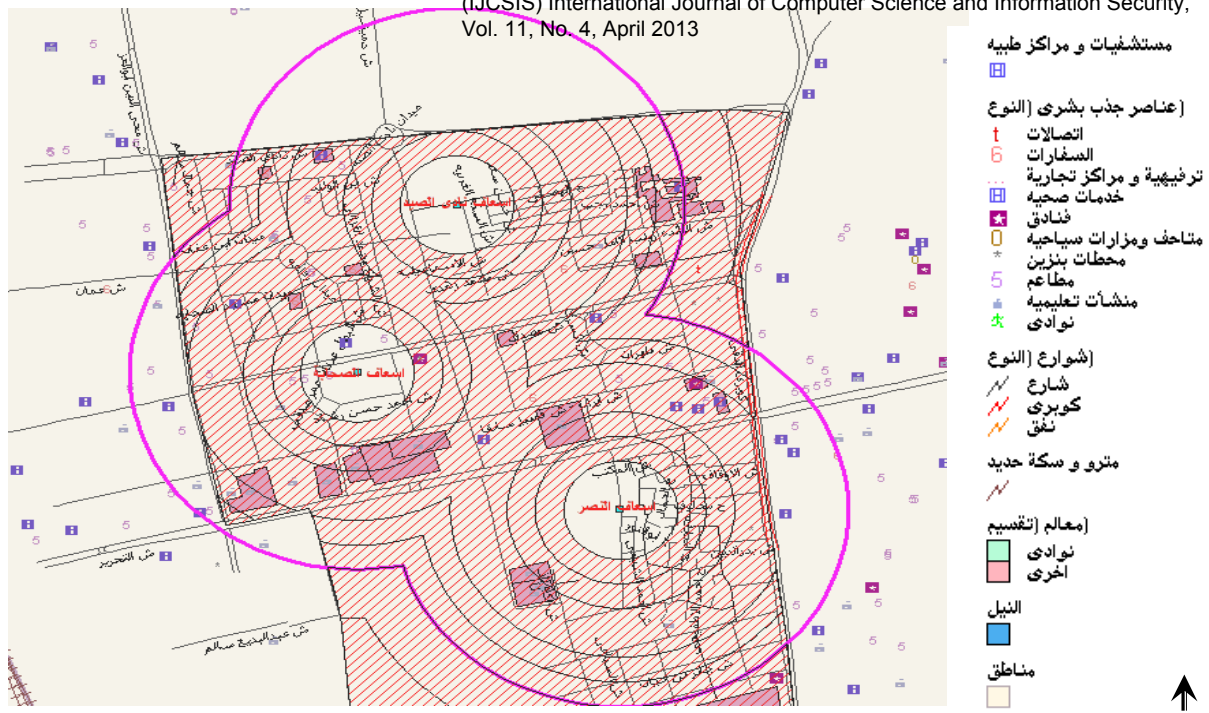


Figure 3. Buffer result showing service area for many health centers

### B. The Application Results Analysis

The main feature in the application is detecting the shortest path between any two points (locations) and return to destination location .

To analyze the results and assure that the drawn shortest path is the actual shortest path, the measure tool provided by application allows giving the accurate exact length between any two vertices by marking a start vertex on the map and following any street line until reaching the stop vertex.

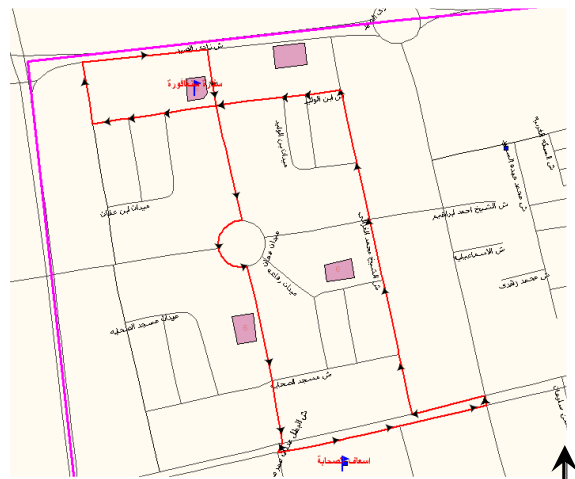


Figure 4. Shortest path between two points and return

Also the application can simulate real time system by change the path until if the path not shorter when the short path contain any problem like crowded or other, system manually by adding point or more between host and destination and system automatic detect a new path as shown in figure (4)

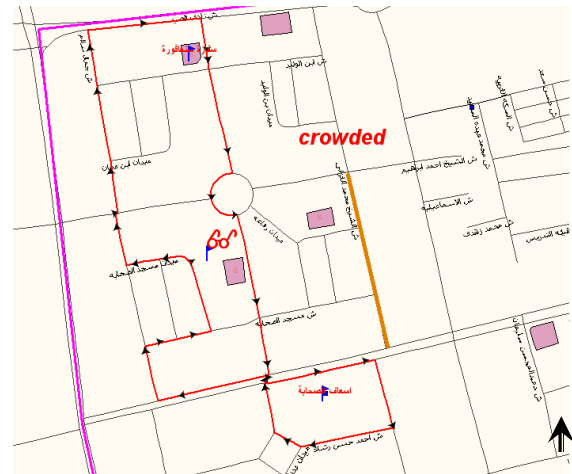


Figure 5. alternative path after system detect crowded street.

The application can also Translates directed path to understand text as turn right or left or derive with street distance (Road topology) and save path as image or text to save time, effort and cost.

### V. CONCLUSION

The problem in the Emergency urgent management is not lack of technology or existence of the relevant information, but often the lack of accessibility of the information  
 Crises and disasters require an accurate and a timely responsive decision support system. And



with the aid of spatial information and map visualization it became much easier to effectively produce an optimal evacuation path, would ambulances be able to follow established transport routes or be diverted to staging areas for casualty collection.

The goal of the GIS is that an end user with a particular background and level of experience can successfully gain insights through a model of the spatial components

The main contribution of this paper is that it represents assessment, planning and decision-making system on GIS platform that combines both spatial analyst as information retrieval, thematic mapping, spatial measurement, overlay, buffer and corridors and network analyst tools functionalities in one framework which is maintainable, usable, scalable, effective, and easy to use.

As a future work, the system will use real-time traffic density data instead of the assumed data with the help of real-time traffic surveillance depends on weather variables and road conditions such as crowd and traffic congestions since the shortest route would be different based on traffic density data; the shortest route is not always the fastest based on its traffic condition..

More evaluation methods and analytics should be performed to widely evaluate the system.

Update system to web based application and mobile application.

## REFERENCES

- [1] Lingyun Zhu, Wenhua Song, Qinggong Li, "Construction of Emergency Decision System Based on GIS," Tianjin Polytechnical University, Tianjin, China, 2009.
- [2] Anhong Ling, Xiang Li, Wenjuan Fan, Ning An, Jian Zhan, Lian Li, Yongzhong Sha, "Blue Arrow: A Web-Based Spatially-Enabled Decision Support System for Emergency Evacuation Planning," School of Information Science and Engineering, Lanzhou University, Lanzhou, China, 2009.
- [3] GIS and Risk-GIS: Decesion Support Tools:  
<http://dssresources.com/dssbook/ch1sbdm.pdf> (last accessed: 25/07/2012).
- [4] CHEN Tao, YUAN Hong-yong, YANG Rui, and CHEN Jianguo, "Integration of GIS and Computational Models for Emergency Management," Center for Public Safety Research, Department of Engineering Physics, Tsinghua University, Beijing, P.R.China, 2008.
- [5] D. Hormdee, W. Kanarkard, and W. Taweepworadej, "Risk management for chemical emergency system based on GIS and Decision Support System (DSS)," Department of Computer Engineering, Khon Kaen University, Thailand, 2006.
- [6] Yang Bo, Wu Yong-gang, Wang Cheng, "A Multi-Agent and GIS Based Simulation for Emergency Evacuation in Park and Public Square," Huazhong University of Science and Technology, Wuhan, China, 2009.
- [7] Zou Zhichong, Wang Yaowu, "Framework of Spatial Decision Support System for Large-Scale Public Building Evacuation," Harbin Institute of Technology, Harbin, China, 2009.
- [8] Gwang-Gook Lee, Byeoung-su Kim, Kee-Hwan Ka, Hyoung-ki Kim, Ja-Young Yoon, Jae-Jun Kim, Whoi-Yul Kim, "Prototype Development of a Spatial Information Management System for Large-scale Buildings," Department of Electrical and Computer Engineering, Department of Sustainable Architectural Engineering Hanyang University, Korea, 2008.
- [9] Wei Jian-guo, Zheng Jian-long, "Research and Development on the Expressway Emergency Response System based on GIS," School of Traffic and Transportation Engineering, Changsha University of Science& Technology, Changsha, China, 2009.
- [10] Carla Willis, Brian van Wilgen, Kevin Tolhurst, Colin Everson, Peter D'Abreton, Lionel Pero and Gavin Fleming, "The Development of a National Fire Danger Rating System for South Africa," Department of Water Affairs and Forestry Pretoria, Pretoria, July 2001.
- [11] Ivan A. Csiszar, "Assessment of the status of the development of the standards for the Terrestrial Essential Climate Variables," Global Terrestrial Observing System, vol. 27, Rome, 2009.
- [12] Wei Jian-guo, Zheng Jian-long, "Research and Development on the Expressway Emergency Response System based on GIS," School of Traffic and Transportation Engineering, Changsha University of Science& Technology, Changsha, China, 2009.
- [13] Han-tao ZHAO, Hong-yan MAO, "Highway Emergency Response System Based on GIS-T," School of Automobile Engineering, Harbin Institute of Technology, Weihai, China, 2009.
- [14] Ivan A. Csiszar, "Assessment of the status of the development of the standards for the Terrestrial Essential Climate Variables," Global Terrestrial Observing System, vol. 27, Rome, 2009.
- [15] Esri-Company History, <http://www.esri.com/aboutesri/about/history.html> (last accessed: 25/07/2012).
- [16] ArcGIS® Spatial Analyst Overview,  
<http://www.rockware.com/product/featuresLobby.php?id=193&category=615> (Last accessed: 25/07/2012).
- [17] ArcGIS® Network Analyst, Overview,  
<http://www.esri.com/software/arcgis/extensions/networkanalyst> (last accessed: 25/07/2012).
- [18] Spatial Analysis: Map overlay and analysis,  
[http://www.geog.ucsb.edu/~kclarke/G176A/2005Lab5/lab\\_5.html](http://www.geog.ucsb.edu/~kclarke/G176A/2005Lab5/lab_5.html) (last accessed: 25/07/2012).
- [19] Algorithms used by Network Analyst,  
[http://webhelp.esri.com/arcgisdesktop/9.3/index.cfm?TopicName=Algorithms\\_used\\_by\\_Network\\_Analyst](http://webhelp.esri.com/arcgisdesktop/9.3/index.cfm?TopicName=Algorithms_used_by_Network_Analyst) (last accessed: 25/09/2012).

## A new technique to accelerate point multiplication specifically for a National Institute of Standards and Technology (NIST) recommended prime field p521

Anil kumar M. N  
Research Scholar  
PET Research Foundation  
PESCE, Mandya

V. Sridhar  
Professor, Department of E&C  
PET Research Foundation  
PESCE, Mandya

**Abstract:** In this paper we propose a new technique to accelerate point multiplication of NIST recommended prime field p521 when the point multiplication is computed by the instruction sets of general purpose microprocessors. We modified the Binary Inversion Algorithm used to compute the inversion which is the costliest operation among other arithmetic operations in point multiplication. Our modified Binary Inversion Algorithm reduces approximately 2,03,286.49 addition operations during a point multiplication when computed by binary scalar point multiplication algorithm. The effectiveness of the above method is analyzed by using statistical analysis. The analysis shows that our technique speeds up the inversion operation and consequently the scalar point multiplication of the NIST recommended prime field p521.

**Key words:** Elliptic curve cryptography, Binary Inversion Algorithm, GF (p) arithmetic operators.

### I. INTRODUCTION

The data security, authentication and integrity have become an essential and urgent need for health care information, confidential communication, storage and financial services etc. The public key cryptosystem is the most efficient method to secure data transaction and messaging. The challenge to implement the most popular public key cryptosystem, RSA is the growing key size. Elliptic Curve Cryptography (ECC) has been considered an alternative to RSA. A lot of implementations have been reported in [1-5]. The advantage of using elliptic curve is that it provides same security level with shorter keys than in RSA. It is estimated that security level of 160 and 224 bits ECC cryptosystem is equivalent to the 1024 and 2048 bits RSA respectively. The research on different algorithms and hardware accelerations have targeted on efficient implementation of elliptic curve scalar point multiplication  $Q=k.P$  which is the fundamental operation of all elliptic curve cryptosystems.

Commonly used Finite Fields are : Finite Field over a large prime called as *Galois Field*  $GF(p)$  and Extended Binary Field that is known as *Galois Field*  $GF(2^k)$ . A very few hardware implementations of ECC on  $GF(p)$  have been reported in the literatures compared to implementations on  $GF(2^k)$  [6-10]. A low power

flexible  $GF(p)$  ECC processor has been reported in [11] which is suitable for RFID tags, wireless sensors and smart cards. A flexible ECC processor over  $GF(p)$  has been reported in [12] which supports all five NIST primes with size ranges from 192 to 521. They have used NAF scalar multiplication algorithm and BIA to compute the inversion. [13] has reported Dual field processors and the design framework for ECC by using mixed projective-affine coordinates which replaces the field inversion. Parallelization of high speed ECC accelerators have been studied in [14].

The hardware complexity to implement ECC in  $GF(p)$  is slightly higher than that of in  $GF(2^k)$  but the advantage is that the k-bit arithmetic unit is capable to process any i-bit data where  $1 \leq i \leq k$ . The arithmetic operations of  $GF(p)$  can be performed faster than  $GF(2^k)$  with the instructions of general purpose microprocessors. Designs in binary fields limit the flexibility and may not be used for Elliptic Curve Digital Signature Algorithm. This algorithm in addition to EC point operation is based on normal integer modulo operations. For binary field designs these modulo operations have to be computed separately by using a processor or in a separate hardware. Inversion is the costliest operation among all the modular operations. Inversion operation can be eliminated with projective coordinate systems with the cost of using parallel multipliers [13-14]. But in small devices like smart cards where area is a constraint, adding more multiplier units needs more memory and thus increases the cost. Speeding up inversion operation is one of the focus of researches in both fields because inversion is the most time consuming operation when affine coordinates are selected.

In this paper we have modified the BIA over  $GF(p)$  to speed up the inverse computation and consequently scalar point multiplication of NIST recommended prime field with modulus  $2^{521} - 1$ . The rest of the paper is organized as follows. Section II provides a mathematical background of ECC. Section III explains about the methodology and in section IV results are discussed. Finally conclusion is given in section V.

### II ECC BACKGROUND

The elliptic curve arithmetic is defined over Galois field  $GF(p)$  where p is a prime number greater than 3. All arithmetic operations are modulo p. The elliptic curve

equation E over GF(p) is given by  $y^2 = x^3 + ax + b$ ; where  $p > 3$ ,  $4a^3 + 27b^2 \neq 0$ , and  $x, y, a, b \in \text{GF}(p)$ . There is also a single element named the point at infinity or the zero point denoted O, which serves as the additive identity. For any point  $P(x, y) \in E$ , we have  $P + O = P$ .

#### A Point addition and Point Doubling:

Additions in GF(p) are controlled by the following rules:

$$\begin{aligned} O &= -O \\ P(x, y) + O &= P(x, y) \\ P(x, y) + P(x, -y) &= O \end{aligned}$$

The addition of two different points on the elliptic curve is computed as shown below.

$$\begin{aligned} P(x_1, y_1) + P(x_2, y_2) &= P(x_3, y_3); \text{ where } x_1 \neq x_2 \\ \lambda &= (y_2 - y_1)/(x_2 - x_1) \\ x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

The addition of a point to itself (point doubling) on the elliptic curve is computed as shown below

$$\begin{aligned} P(x_1, y_1) + P(x_1, y_1) &= P(x_3, y_3); \\ \lambda &= (3x_1^2 + a)/(2y_1) \\ x_3 &= \lambda^2 - 2x_1 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

#### B Point Multiplication:

Scalar multiplication  $Q = k.P$  is the result of adding point P to itself (k-1) times

$$Q = k.P = P + P + \dots + P. \\ (k-1 \text{ Times})$$

The binary method is the simplest and oldest efficient method for point multiplication. It is based on the binary expansion of k. The corresponding algorithm is shown below.

INPUT: A point P and an integer k

OUTPUT:  $Q = k.P$

1.  $Q \leftarrow P$
2. For  $j = L-2 \dots 1, 0$ 
  - 2.1  $Q \leftarrow 2Q$
  - 2.2 IF  $k_j = 1$  THEN  $Q \leftarrow Q + P$
3. RETURN Q

Algorithm 1: Binary scalar multiplication algorithm

Another commonly used algorithm is NAF scalar multiplication algorithm which is shown below.

INPUT: A point P and an integer k, NAF k with no leading 0's

OUTPUT:  $Q = k.P$

1.  $Q \leftarrow P$
2. For  $j = |k| - 2 \dots 1, 0$ 
  - 2.1  $Q \leftarrow 2Q$
  - 2.2 IF  $k_j = 1$  THEN  $Q \leftarrow Q + P$   
IF  $k_j = -1$  THEN  $Q \leftarrow -Q + P$
3. RETURN Q

Algorithm 2 NAF scalar multiplication algorithm

If we assume that, on average 'n' is the number of ones in 'k' which is equal to  $n = L/2$ , the binary method requires  $(L-1)$  point doublings and n point-additions where L denotes the number of bits of the prime p. The point doubling and point addition require one inversion operation. Hence the average number of inversion operations required during a point multiplication with the prime p521 is equal to  $521 + (521-1)/2 = 781$

With the NAF scalar point multiplication the average number of inversion operations required during a point multiplication with the prime p521 is equal to  $521 + (521-1)/3 = 694.33$

### III. METHODOLOGY

Speed up in computation of point multiplication is obtained by modifying the Binary Inversion Algorithm by replacing the two 'addition and division by 2' operations of steps 2.1.2 and 2.2.2 by Rotate Right operations. The  $x_1 = (x_1 + p)/2$  operation of step 2.1.2 and  $x_2 = (x_2 + p)/2$  operation of step 2.2.2 of Binary Inversion Algorithm are replaced by Rotate  $x_1$  right by 1 bit (ROR $x_1$ ) and Rotate  $x_2$  right by 1 bit (ROR $x_2$ ) operations. Division by 2 is achieved by shifting right the operand right by one bit. Since the rotate and shift operation take same time for execution, we have saved the time for addition of two 521-bit numbers. This replacement is possible only if the prime is a Mersenne's prime thus removing two 521-bit addition operations from the Binary Inversion Algorithm. The Binary Inversion Algorithm and modified Binary Inversion Algorithm are shown in figure 2.1 and 2.2 respectively.

INPUT: Prime p and  $b \in [1, p-1]$

OUTPUT:  $b^{-1} \bmod p$

1.  $u = b, v = p, x_1 = 1, x_2 = 0$
2. while (u != 1 and v != 1) do
  - while u is even do
    - 2.1.1  $u = u/2$
    - 2.1.2 if  $x_1$  is even then  $x_1 = x_1/2$   
else  $x_1 = (x_1 + p)/2$
    - 2.1.3 end while
  - 2.2 while v is even do
    - 2.2.1  $v = v/2$
    - 2.2.2 if  $x_2$  is even then  $x_2 = x_2/2$   
else  $x_2 = (x_2 + p)/2$
    - 2.2.3 end while
  - 2.3 if  $u \geq v$  then  $u = u - v, x_1 = x_1 - x_2$   
else  $v = v - u, x_2 = x_2 - x_1$
- 2.4 end while
- 2.5 if (u == 1) return  $x_1 \bmod p$  else  
return  $x_2 \bmod p$

Fig 2.1: Binary Inversion Algorithm

```

INPUT: Prime p and b  $\in [1, p-1]$ 
OUTPUT:  $b^{-1} \bmod p$ 
1.  $u=b, v=p, x1=1, x2=0$ 
2. while (u  $\neq 1$  and  $v \neq 1$ ) do
    2.1 while u is even do
        2.1.1  $u = u/2$ 
        2.1.2 if x1 is even then  $x1 = x1/2$ 
            else  $x1 = \text{ROR } x1$ 
        2.1.3 end while
    2.2 while v is even do
        2.2.1  $v = v/2$ 
        2.2.2 if x2 is even then  $x2 = x2/2$ 
            else  $x2 = \text{ROR } x2$ 
        2.2.3 end while
    2.3 if  $u \geq v$  then  $u = u - v, x1 = x1 - x2$ 
        else  $v = v - u, x2 = x2 - x1$ 
    2.4 end while
    2.5 if (u==1) return  $x1 \bmod p$ 
        else return  $x2 \bmod p$ 

```

Fig 2.2: Modified Binary Inversion Algorithm

#### IV RESULTS AND DISCUSSIONS

The proposed method of replacing the addition operations in the computation of inversion has been applied in the software environment where point multiplication is computed by instruction sets of general purpose microprocessors. When the point multiplication is computed using the instruction sets of general purpose microprocessors or microcontrollers which do not support instruction level parallelism, significant number of addition operations have been eliminated. This has been justified with statistical analysis.

Because of the infeasibility to process with the whole number space of the Mersenne's prime  $2^{521}-1$ , statistical analysis has been done with the same Mersenne's primes mentioned in the previous section and some part of number space of the Mersenne's prime  $2^{521}-1$ . The effectiveness of the proposed method in the software domain has been concluded on the basis of the number of the addition operations reduced during the computation of inversion operations when the point multiplication is performed. Results have been tabulated for binary point multiplication and NAF point multiplications algorithms.

Table 1 shows the average number of addition operations reduced during the computation of inversion with different Mersenne's primes

Table 1 Analysis with different Mersenne's primes

Mersenne's Prime	Total Number of additions operation reduced with all numbers in the range 1 to (p-1)	Average number of addition operations reduced during the computation of one inversion
$2^5-1$	55	1.833
$2^7-1$	327	2.5952
$2^{13}-1$	46840	5.71
$2^{17}-1$	1052272	8.028
$2^{19}-1$	4809285	9.17
$2^{31}-1$	$3.23165047 \times 10^{10}$	15.0485

Analysis has been carried out to some parts of the number space of Mersenne's prime  $2^{521}-1$  which is show below.

Table 2. Parts of number space showing the region of analysis carried out

Number space
$(p-1)/2+1$ to $(p-1)/2+1+2^{17}$
$(p-1)/2+2^{127}$ to $(p-1)/2+2^{127}+2^{17}$
$(p-1)/2+2^{250}$ to $(p-1)/2+2^{250}+2^{17}$
$(p-1)/2+2^{350}$ to $(p-1)/2+2^{350}+2^{17}$
$(p-1)/2+2^{500}$ to $(p-1)/2+2^{500}+2^{17}$

Average number of addition operations reduced during the computation of one inversion = 260.29.

The results obtained shows that the average number of addition operations reduced during the computation of one inversion operation is half of the number of bits of the Mersenne's prime as Mersenne's primes becomes higher and higher which is justified with the results obtained which is tabulated in Table 3.

Table 3. Relation between the bit length of Mersenne's primes and average number of reduced addition operation..

Mersenne's Prime	Bit Length	X=Average number of addition operations reduced during the computation of one inversion	Bit length/X
$2^5-1$	5	1.833	2.7277
$2^7-1$	7	2.5952	2.69
$2^{13}-1$	13	5.71	2.27
$2^{17}-1$	17	8.028	2.1175
$2^{19}-1$	19	9.17	2.07
$2^{31}-1$	31	15.0485	2.06
$2^{521}-1$	521	260.29	2.0016

The result tabulated in the last row is the result of analysis conducted on the selected part of the number space of Mersenne's prime  $2^{521}-1$ . The number of addition operations reduced during a point multiplication with two scalar point multiplication algorithm with the Mersenne's prime  $2^{521}-1$  is shown in table 4.

Table 4. Number of addition operations reduced during a point multiplication with different point multiplication algorithms

Point multiplication algorithm	Average number of inversion operations required to compute one point multiplication	Average number of addition operations reduced during the computation of one inversion operation	Average number of addition operations reduced during the computation of one point multiplication
Binary scalar algorithm	781	260.29	2,03,286.49
NAF scalar algorithm	694.33	260.29	1,80,727.15

## 5. CONCLUSION AND FUTURE SCOPE

We have presented a new technique to speed up the computation of scalar point multiplication in software domain by modifying the Binary Inversion Algorithm. The effectiveness of the technique is analysed by statistical analysis with Mersenne's prime  $2^{521}-1$  and with other Mersenne's primes. The result show that modified BIA has reduced on average 2,03,286.49 addition operations when point multiplication is computed by Binary point multiplication algorithm.

Because of the infeasibility to process whole number space with Mersenne's prime  $2^{521}-1$ , the result obtained is an approximation of the accurate result and hence more simulations have to be carried out to achieve more accurate results. Our future effort will target speeding up computation of individual computational blocks of scalar point multiplication, and the integration of the computational blocks to achieve better performance.

## REFERENCES

- [1].C. McIvor, M.McLoone and J.V.McCanny, "Modified Montgomery modular multiplication and RSA exponentiation techniques", IEE Proc. Comput.Digit.Tech., Voi.151,N9.6, November 2004
- [2]QIANG Liu, Fangzhen Ma, Dong Tong, Xu Cheng, "A regular Parallel RSA Processor", The 47<sup>th</sup> IEEE

International Midwest Symposium on Circuits and Systems.

- [3]Jin Hua Hong, Cheng-Wen Wu, "Cellular-Array Modular Multiplier for fast RSA Public-Key Cryptosystem based on modified Booth's Algorithm", IEEE Transactions on VLSI systems, Vol.11, No.3, June 2003.

- [4]Andre Vandemeulebroecke, Etienne Vanzieleghem, Tony Denayer, Paul G, "A new carry free division algorithm and its application to a single chip 1024-b RSA processor", IEEE Journal of Solid State Circuits, Vol.25, No.3, June 1990.

- [5]Ming-Der Shieh, Jun-Hong Chen, Hao-Hsuan Wu, Wen-Ching Lin, "A new modular exponentiation architecture for efficient design of RSA cryptosystem", IEEE Transactions on VLSI systems, Vol.16, No.9, September 2008.

- [6].William N Chelton, Mohammed Benaissa, "Fast Elliptic Curve cryptography on FPGA", IEEE Transactions on VLSI systems, Vol.16, No.2. February 2008.

- [7]. William N Chelton, Mohammed Benaissa, "Design of Flexible  $GF(2^m)$  Elliptic Curve Cryptography Processors", IEEE transactions of VLSI systems, Vol.14, No.6, June 2006.

- [8].Ray C.C. Cheung, Nicolas Jean-baptiste Telle, Wayne Luk, Peter Y.K. Cheung, "Customizable Elliptic Curve Cryptosystems", IEEE Transactions on VLSI systems, Vol.13, No.9, September 2005.

- [9].Alireza Hodjat, David D. Hwang, Ingrid Verbauwhede, "A scalable and high performance elliptic curve processor with resistance to timing attacks", ITCC'05.

- [10]Philip H. W. Leong, Ivan K.H.Leung, "A Microcoded Elliptic Curve Processor using FPGA Technology", IEEE Transactions on VLSI systems, Vol.10, No.5, October 2002.

- [11]. Hamid Reza Ahmadi, Ali Afzali-Kusha, "Low-power flexible  $GF(p)$  Elliptic curve cryptography processor",

- [12]. Kendall Ananyi, Hamad Alrimeigh, Daler Rakhmatov, "Flexible hardware processor for Elliptic curve cryptography", IEEE transactions on VLSI systems, Vol.17, No.8, August 2009.

- [13]. Jyu-Yuan Lai, Chih-Tsun Huang, "Elixir: High throughput cost effective dual field processors and the design framework for ECC". IEEE Transactions on VLSI systems, Vol.16, No.11, October 2008

- [14]. Kimmo Jarvinen, Jorma Skytta, "On parallelization of High-speed processors for

Ellipticcurve cryptograpy”, IEEE Transactions on



Anil Kumar M N is a research scholar at PET Research Foundation, PESCE, Mandya. He is currently pursuing his Ph.D from University of Mysore. His research area includes cryptography.

VLSI systems, Vol.16, No.9, September 2008



V Sridhar is a Professor at the department of Electronics and Communication, PESCE, Mandya and currently is the Principal of PESCE, Mandya. He has 30 years of teaching and research experience. He has published around 40 research papers in various national and international journals. His research areas include Biomedical Signal Processing, VLSI and Cryptography.

# A Novel Agent based Communication in Wired - WIMAX Hybrid Network in MANET

Kalyani chaturvedi  
M.TECH (EC.deptt.)

Truba institute of engineering and information technology  
Bhopal, India

Neelesh Gupta  
H.O.D Dept. Of EC

Truba institute of engineering and information technology  
Bhopal, India

**Abstract**— Wireless technologies are able to provide mobility and portability that makes it more attractive as compared to wired technologies. Further, increasing requirement to support exiting connectivity with higher data rate for mobile computers and communication devices are performing a significant role to growing interest in wireless networks. WIMAX (Worldwide Interoperability for Microwave Access) is a telecommunications protocol that gives fixed and fully mobile internet access. This paper presents the role WIMAX technology in MANET at MAC layer. Wired network refers to interoperable implementations of the IEEE 802.3 and WIMAX which refers to interoperable implementations of the IEEE 802.16 wireless-networks standard. The radio range and data rate of WIMAX are much better than Wired network but, on the basis of cost WIMAX is expensive. In this paper is just proposal of a new hybrid network that is the communication between two different technologies on the basis of novel Agent, Wired Node (WN) and Mobile Node (MN). Now the Agent is worked as a interface in between wired and WIMAX network and Agent is connected with wired network to synchronize the communication with WIMAX, first the request is goes to Agent then to network. The combinations of these two technologies are not very expensive and also better than wired. In previous there is no such work done on Wired-WIMAX hybrid network. Their performance will be measure on the basis of TCP congestion window.

**Keywords**- Wired Network, Agent, WN, MN, WIMAX, MAC, MANET, TCP.

## I. INTRODUCTION

In use of without fixed infrastructure nodes are communicate with each other in mobile communication. These networks have no fixed routing nodes. All nodes are capable of movement and can be connected in any random manner. These networks are mainly used in disaster or emergency areas where no prior fixed infrastructure exists. One of the challenging aspects in these ad hoc networks is to find and develop routing protocols that can efficiently find routes between any two nodes. The routing protocol should take into account the mobility factor in these networks and the topology being used. For this reason, performance evaluation of various protocols has been carried out by different authors. In [1], performance of Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector Routing (AODV) has been considered. The performance is analyzed using various network load, mobility and network size. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) is another protocol which is

a table-driven protocol used in wireless networks [2]. Various performance parameters for these protocols have been explored including packet end to end delay etc. Rest of the portion of paper is summarized as, section 2 presents the overview of WIMAX technology and section 3 is of related work. Routing procedure of AODV Protocol is described in Section 4. Section 5 and section 6 is of problem statement and proposed work. In this paper simulation result and conclusion are present in section 7 and section 8.

## II. WIRED -WIMAX TECHNOLOGY

Wired Local Area Networks make use of Ethernet cables and network adapters. Numerous computers can be wired to one another by using an Ethernet crossover cable. Wired LANs also need vital devices like hubs, switches, or routers to aid further computers.

- 1) For dial-up connections to the Internet, the computer hosting the modem should administer Internet Connection Sharing or similar software to share the connection with every other computer on the network.
- 2) Broadband routers permit easier sharing of cable modem or DSL (Dynamic source load) Internet connections, furthermore they often include built-in firewall.
- 3) Ethernet cables should proceed from each computer to a different computer or to the central device.
- 4) The accurate cabling configuration for a wired LAN differs depending on the merge of devices, the form of Internet connection.
- 5) Following hardware installation, the lasting steps in configuring either wired or wireless LANs do not contrast a great deal. Equally rely on standard Internet Protocol and network operating system Configuration options.

All wired networks differ from each other. The most familiar type of wired network is an Ethernet network.

In wired networking cabling (wired Ethernet as defined by IEEE 802.3) consists of 4 pairs of copper cabling that can be utilized for both voice and data transmission. If we use reduce crosstalk and electromagnetic induction use two wire twisted together. The transmission speed ranges from 2 million bits per second to 10 billion bits per second.

Twisted pair cabling comes in two forms: unshielded twisted pair (UTP) and shielded twisted-pair (STP). Each form comes in several category ratings, designed for use in various scenarios

The original standard which allows for a 70Mbps speed at distances of up to 30 miles using the 10GHz and 66GHz bands. 802.16e: This standard is the newest standard and employs the 2GHz and 6GHz bands. This standard allows mobile devices to use wireless technology. The 802.16e-2005 standard was developed under IEEE guidelines, but the implementation was left to private industry. The WIMAX Forum was created to solve interoperability problems and promote the standard itself [4].

WIMAX is an abbreviation for Worldwide Interoperability for Microwave Access and its architecture is based on broadband point-to-multipoint wireless access [5]. WIMAX was created in 2001 to promote the IEEE802.16 standard. This standard was finally approved in June 2004 [14]. The 802.16 standard provides for fixed and mobile WIMAX in 802.16d and 802.16e, respectively. Some important characteristics of WIMAX include:

- 1) Its use of the microwave frequency band for wireless data transmission
- 2) Its high transmission speed over long distances.
- 3) its use of OFDM (Orthogonal Frequency Division Multiplexing) to enable non-line-of sight communication.
- 4) Its multi-channel support for TDD (Time Division Duplex) and FDD (Frequency Division Duplex)
- 5) Its flexible handling of channels in the 3.5MHz, 5MHz and 10MHz frequencies. Some challenges for WIMAX include:
  - a. Reaching a coverage area of up to 10 miles.
  - b. Providing wireless broadband and dedicated links.
  - c. Making the technology more affordable.
  - d. Allowing access from more remote areas.

Although WIMAX technology is relatively new, its brief history and development consists of four phases [4]. Comparison of Wired-WIMAX network shown in table.1 On the basis of following constraint WIMAX has definitely superior than wired. Due to the excellent performance, WIMAX are also very costly and wired cost is not too much. So on the basis of cost and other constant their hybrid network are definitely show the good performance.

**TABLE I**  
**CONSTRAINT BASED COMPARISON OF TWO TECHNOLOGIES**

Constraint	Wired Network	WIMAX Network
Installation	Moderate difficult	Easier, but beware interfaces
Cost	Less	More
Reliability	Moderate	Reasonably high
performance	Good	Very good
Security	Reasonably good	Reasonably good
Mobility	Limited	Outstanding

### III. RELATED WORK

On the basis of previous observations, no work is done on Wired-WIMAX hybrid network. Hybrid is a network in which two different technology are combined. In hybrid network communication between the two different technologies are possible and also examine their performance on the basis results.

There are no kind of work is done on Wired -WIMAX network but some work is done on Wi-Fi-WIMAX network this section give details of that work.

In December, 2001, the Wireless MAN-SC [3] standard was established. This standard specifies the physical layer and multichannel techniques, including the single-carrier that can handle both TDD and FDD.

In 2003, WIMAX was consolidated under the IEEE 802.16a standard to support OFDM in the PHY layer. During this time substantial changes were made to the 802.16a standard, resulting in the 802.16c standard. The 802.16c standard is the basis of HIPERMAN (High Performance Metropolitan Area Network); and of 802.16e-2005, which specifies scalable OFDM for the PHY layer. As already mentioned, the WIMAX standard is divided into several sub-standards 802.16a and so on. A novel approach for the measurement and estimation of aggregate traffic in Local Area Network environment has been discussed in [18]. The addition of a switch with a hub's network makes a network perform better in terms of throughput and delay characteristics [19].

IEEE 802.16(WIMAX) technology [6] has been proposed to overcome the critical problems of WLANs [7] and cellular networks. It provides greater coverage area and better mobility support while encouraging high transmission rate. In addition, it also supports heterogeneous traffic by means of various QoS scheduling. WIMAX also provides a solution for scenarios that are too remote to receive internet access via cable or DSL.

The WIMAX technology can be used for creating a wide-area wireless backhaul network. With the deployment of backhaul-based WIMAX many value added services can be provided to the service area.

To efficiently support the large number of customers in the WIMAX network, the network can be enabled with distributed services [9]. In other words, a customer can access the particular service from any of the servers in the network in which the servers are distributed to serve the entire metropolitan area. In this method, the customer does not specify the exact address of the server in the network which runs the particular service; whereas it only indicates the service it wants to access.

In this paper [15] proposed to develop a cross-layer based QoS Routing (CLBQR) Protocol for 802.16 WIMAX networks. In our protocol, the cross layer routing is based on the routing metrics which include power, link quality and end to end delay. Then the routing is performed by estimating the combined cost value of these metrics. In this simulation result show that our proposed protocol achieve higher packet delivery ratio with less energy consumption and delay.

By using the Author EETT (Exclusive Expected Transmission Time) metric to approximate the link quality .IN this method of EETT use to give better estimate of multi



Channel path.. The end-to-end delay of a packet is the time it takes to travel from source node to destination node including intermediate links transmission delays and nodes, queuing delays. For the estimation of queuing delay, we use the average queuing delay to each node. Our protocol is the derivatives of the AODV routing protocol which is the variant of classical distance vector routing algorithm. Then the routing is performed based on the routing metrics by estimating a combined cost value.

In this paper [16], when the RREQ and RREP message are generated or forwarded by the nodes in the network each node appends its own address on this route discovery message. In a certain point the RREQ packet contain a list of all the nodes traversed. Each node also updated its routing table with all the information contains in the control message. The protocol, AODV-SRA, merge source route path accumulation during the route discovery process in AODV to attain extra routing information. The number of routes accumulated in AODV-SRA increases the number of nodes and connections. This is because the number of route accumulates the route discovery increases as the number of node increase. The size of the control packets in the AODV-PA protocol is larger than that of AODV. This is compensated by the decrease in the number of routing packets in AODV-PA could also be suitable either if overall routing load or if application oriented metrics such as delay and packet delivery ratio are important for the ad hoc network application.

Using 4G Wireless scenario, OFDM and WI-MAX are Long Term Evolution standard. In this article, we do a detailed comparison of the implementation of OFDMA in LTE and WIMAX. This article [17] has compared the use of OFDMA in WIMAX and LTE standards in detail. Both systems leverage many facets of OFDMA, including frequency diversity and frequency and time axes granularity. Subtle differences in exploiting different advantages of OFDMA in both systems are highlighted. Note that the physical layer overhead is higher for WIMAX systems than for LTE.

When number of communication high in AODV and DSR drop the performance at high velocities. By this method previous work [10] has studied the performance of AODV and DSR in a variety of scenarios. This work showed that both AODV and DSR drop in performance at high velocities or when the number of connections is high. In simulation result , the authors proposed modifications to AODV that could improve the performance of each protocol. One of the main proposals is the accumulation of the source route in request and reply packets during the route discovery process in AODV. By accumulating this information, nodes can increased amount of routing information to different destinations. So the proposed work should lead to a reduction in the routing load of AODV. To evaluate the new protocol, a detailed packet-level simulation comparing the performance of AODV with source route path accumulation to AODV is presented.

In [11], R. Bera et al. present a performance analysis of a university network combining the IEEE 802.11n standard and WIMAX technology. The paper describes the benefits of using these technologies in tandem, even when one of them is recently approved (WIMAX) for certifying purposes and the other is scarcely commercially available (802.11n). The problem related integration of these two technologies document solution are possible or initial. However, the authors themselves recognize that security issues and the lack of availability of adequate equipment for testing the network's performance were significant limitations.

In [12], Shilpa et al. present a comparative study of emerging WIMAX, 3G, and Wi-Fi wireless technologies. The authors describe the main characteristics of these technologies, as well as the advantages and disadvantage of each of them. Their paper, however, is theoretical in nature and does not provide quantitative results based on simulations. Currently, Wi-Fi-WIMAX integration is based on the IEEE802.16d protocol, also known as Fixed WIMAX. The IEEE 802.16e standard has yet to be deployed because it is still undergoing the certification process. One of the greatest problems is how to solve changing the network nodes that can cause break in the network connection .Consequently, any proposed routing algorithm must allow for highly dynamic nodes and network partitions.

Quality of service (QoS) and mobility are the most common challenges, thus require specific protocols to integrate different types of wireless networks. The most significant problem in terms of QoS is the actual handoff, where nodes must pass information between cells [5].

An important aspect to consider is that the basic support for QoS differs significantly between WLAN and WMAN because of the different architectures, and more specifically, the specifications of their physical and MAC layers [5].

WIMAX technology supports both PMP and Mesh. A WIMAX PMP network provides last mile access to broadband Internet services by organizing the nodes in a manner that is similar to cell phone networks because it uses a BS. Meanwhile, in mesh topology, an ad hoc network functions independently of the BS. Each node can simultaneously transmit and receive information from neighbor nodes. Additionally, they can send information using a multichip strategy to communicate with nodes that are further away. [9]. The integration of Wi-Fi-WIMAX has become increasingly common in urban areas where they work in tandem to provide mobile services and a variety of applications. Presently, several cities are attempting to become "wireless cities" in an effort to provide broadband wireless internet access throughout their entire metropolitan areas. Wi-Fi and WIMAX are two options for internet access in metropolitan networks [9].

Presently, integrating Wi-Fi and Fixed WIMAX is the most practical way to deploy large-scale wireless networks in cities that require wireless broadband connectivity [9]. The most famous Secure Wireless Cities (SWCs) projects include wireless Philadelphia, the San Francisco Tec connect Project, and Google Wi-Fi Mountain View [6, 7, and 8].

The purpose of the Wireless Philadelphia Project is to provide the Philadelphia metropolitan area with wireless services. Handled through Wireless Internet Partners (WIP), even though the entire city does not enjoy full coverage, the goals set by WIP will soon be reached. Although the WIP does not offer its services free of charge, there are some free zones located in public spaces like parks and gardens [6].

San Francisco Techconnect is an initiative for promoting internet services, training, and technical support for the citizens of San Francisco, California. This project places special emphasis on serving low income groups or people with special needs. An important goal of the San Francisco Techconnect project is to promote new applications, contribute to economic growth, and improve municipal services. [7].

The Google Wi-Fi Mountain View project provides free internet to the city of Mountain View, California. The main goal is to provide city-wide service and uses mesh architecture to provide Wi-Fi services [8]. Each project was motivated and developed for different reasons, but most of these projects remain true to offering free internet services to entire cities. The creation of a protocol which allows users access to both types of technologies without problems has great advantages for both users and service providers. Offering integrated WLAN/WMAN services will provide users both performance and high speed data transmission [5]. Ali-Yahiya et al. propose an architecture where the Wi-Fi and WIMAX networks and their traffic routes are separated by dedicated gateways to provide interconnectivity.

#### IV. AD HOC ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL

Ad hoc On-Demand Distance Vector Routing Protocol (AODV) [13] is another reactive routing protocol, which is doing the following procedures:

1. **Route discovery:** If the route is not available in the routing table towards the destination, a RREQ (Route Request) packet is broadcast throughout the MANET with a search ring technique. On receipt of RREQ, the node creates a reverse routing entry towards the originator of RREQ, which is used to forward replies later. The destination or the intermediate node, which has a valid route towards the destination, answers with a RREP (Route Reply) unicast packet. On receipt of RREP, the reverse routing entry towards the originator of RREP is also created, similar to the processing of RREQ. Associated with each routing entry is a so-called precursor list, which is created at the same time. The suggest list contains the upstream nodes which use the node itself towards the same destinations.
2. **Route maintenance:** Every node along an active route periodically broadcasts HELLO messages to its neighbors. If the node does not receive a HELLO message or a data packet from a neighbor for a while, the link between itself and the neighbor is considered to be broken. If the destination with this

neighbor as the next hop is believed not to be far away (from the invalid routing entry), local repair mechanism may be launched to rebuild the route towards the destination; otherwise, a REER (Route Error) packet is sent to the neighbors in the precursor list associated with the routing entry to inform them of the link failure.

#### 3. Route table management

AODV needs to keep route of the following information for each route table entry: x Destination IP Address: IP address for the destination node.

- a) Destination Sequence Number: Sequence number for this destination.
- b) Hop Count: Number of destination included in hopes.
- c) Next Hop: The next, which has been designated to forward packets to the Destination for this route entry.
- d) Lifetime: The time for which the route is Considered valid. Active next list: Neighbor nodes that are actively using this Route entry.
- e) Request buffer: In request buffer that is only processed once.

#### V. PROBLEM STATEMENT

The problem in WIMAX technology is cost and in wired is not possible to provide connectivity in everywhere. WIMAX is also a wireless technology but it will be enhance in radio range and presence of OFDM as compare to Wired. Wired WIMAX communication has no doubt provides better results but have some limitations that has tried to solve by combining Wired and WIMAX hybrid network.

#### VI. PROPOSED WORK

According to problem statement, Wired and WIMAX hybrid network is use to resolve the limitation of wired and WIMAX. The combination of these two technology is not very expensive and is far better than wired and WIMAX alone. In wired and WIMAX technology mobile node is created it uses AODV (ad-hoc on demand distance vector) routing as routing protocol , wireless channel for prorogation type of two ray ground wave because mobile node contain routing table and also node radio range is limited so our data transmitted from node to node after that we apply MAC (media access control technique) as 802.16 WIMAX that provides greater radio range as compare to 802.3 WLAN scheme our dissertation work proposed in WIMAX scheme so here we elaborate WIMAX network.

##### A. Algorithm for AODV Routing Discovery and Scenario Generation with WIMAX standard

Mobile node = N; // Number of mobile nodes

Sender node = S; // sub set of N i.e. MH

Receiver Node = R; //sub Set of N i.e. MH

```
Start simulation time = t0
Set routing protocol =
AODV; Set MAC = 802.16
Set radio range = rr; //initialize radio
range RREQ_B(S, R, rr)
{
If ((rr<=550) && (next hop >0))
{
Compute route ()
{
rtable->insert(ratable->rt_nexthop); // next hop to RREQ
source rtable1->insert(rtable1->rt_nexthop); // next hop to
RREQ destination
if (dest==true)
{send ack to source node with rtable1;
Data_packet_send(s_no, next hop, type)
}
Else {
Destination not found;
}
}
}
Else
{
Destination un-reachable;
}
}
```

#### Communication of Wired with WIMAX on the basis of Agent

Frequency division multiplexing (FDM) is a technique use of 48 KHZ in Wired communication network total bandwidth increased by division technique of frequency.

Multipath interference [11, 18] is a phenomenon used in OFDM (used by Agent) in the technique of where a signals from a source travels to a detector via two or more paths and, under the right condition frequency of 3GHz

```
If (Frequency >48 KHz)
{
```

```
Wired WIMAX communication is possible on the basis of
channel estimation}
```

```
# now channel estimation [11] calculation and channel
equalization [11] on the basis of frequency. So calculate
required frequency for communication in between Time
Division Multiplexing (TDM) and OFDM
```

```
{Calculate required frequency = (difference of frequency of
wired and WIMAX
```

```
Then
```

```
Calculate difference of the frequency range need for
communication for WIMAX and maintain the synchronization
in TDM wired and OFDM WIMAX
```

```
if (check frequency is == possible communication means
(3GH))
```

```
Then
```

```
Data in the foam of signals passes to WIMAX Network
```

```
}
Else
{No synchronization is possible on the basis of
frequency in wired WIMAX}
```

The Wired WIMAX communication are shown in figure 1. This figure represents the one wired topology and one WIMAX mobile node topology. Here WN represents *wired Node*, A communication intermediate is *Agent* attach in wired network and MN represents *Mobile nodes* in wireless network. Basically the wired node functioning is only in wired network means all the WN are free to communicate in wired network without any Agent and Mobile Node are similarly free to do communication in between mobile nodes without any Agent. The main function of Agent is to do the communication in between wired network and WIMAX network. This node is working as an intermediate in between these two networks means only agent having a capability to maintain synchronization in Hybrid Network because Agent understands both network. The communication of Agent with WN and to MN is based on OFDM and TDM.

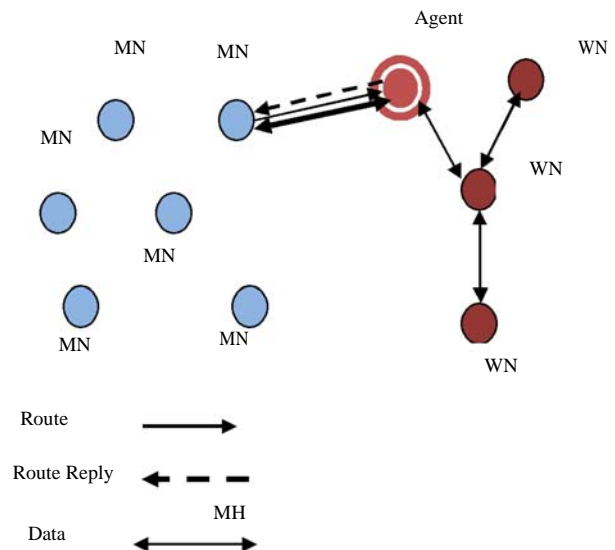


Figure 1 TCP Wired WIMAX communication on the basis of Agent.

#### VII. SIMULATION ENVIRONMENT

NS2 is an open-source event-driven simulator designed specifically for research in computer communication networks. The especially we have used to simulate the ad-hoc routing protocols in is the Network Simulator 2 (ns) [20] from Berkeley. To imitate the mobile wireless radio environment we have used a mobility extension to ns that is developed by the CMU Monarch project at Carnegie Mellon University. Since its inception in 1989, NS2 has continuously gained tremendous interest from industry, academia, and government. On the basis of simulation parameters given in Table 2 simulation has been done in ns-2 simulator.

### A. Simulation Parameters

Simulation has been done in Network Simulator (ns 2.31 version). Here the wired topology are consider three WN and single Agent and connections are established in between MN to WN through Agent i.e. each MN are communicate with WN through Agent. WIMAX wireless ad hoc parameters are shown in table 2.

**TABLE II**  
**SIMULATION PARAMETERS**

Simulator used	NS-2.31
Number of nodes (MH)	21
Dimensions of simulation area	800×800
Transmission range	250m
Network type	802.3 and 802.16
Routing protocol	AODV
Simulation Time	100sec.
Traffic Type (TCP and UDP)	CBR (3pkt/s)
Packet size	512bytes
Nodes Movements	Random
Number of WN and MN	3and 1

### B. Results

In this section we present a set of simulation experiments to evaluate this protocol by comparing with the Communication of WIMAX network and Wired WIMAX Network. The results are calculated on the basis of TCP congestion window in both cases.

#### 1) TCP packet analysis in Wired network

This graph represents the analysis of TCP packets in case of wired communication. In wired communication the maximum packets are delivered are 16 in a given simulation time. In this graph the three connections are created and measures the performance of wired communication network.

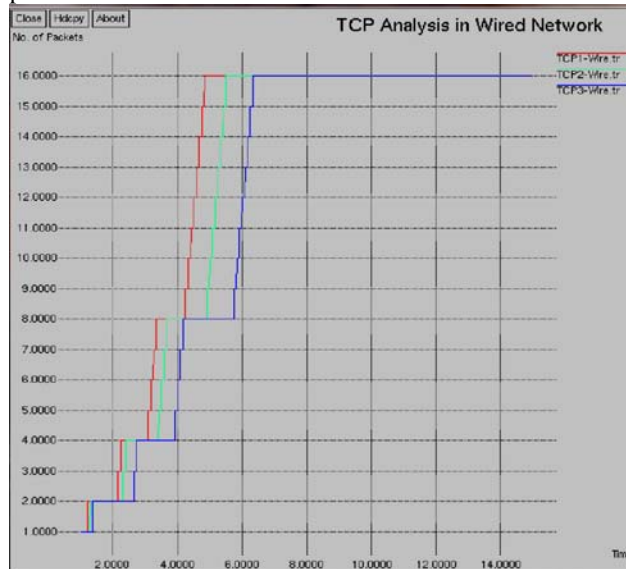


Figure 2 TCP Analysis in wired network.

#### 2) TCP packet analysis in WIMAX network

In this graph the number of connections represents the data and acknowledgement information of packets. In this graph

We clearly visualized the in only WIMAX communication the maximum packets are delivered 65 in a given simulation time. The number of packets in rest of the connections are not deliver properly the window size are varies rapidly and also small by that less number f packets are deliver.

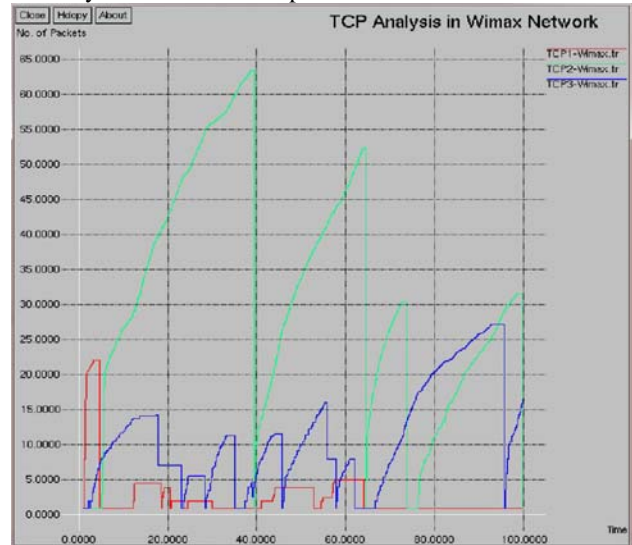


Figure 3 TCP Analysis in WIMAX network.

#### 3) TCP packet analysis in Wired-WIMAX network

In this graph we show the analysis of TCP packets in case of Wired-WIMAX communication. Here we clearly visualized that the maximum size of window is 60 and 65, which is slightly greater then WIMAX communication. In this graph we only compare the performance of highest packet deliver TCP connections.

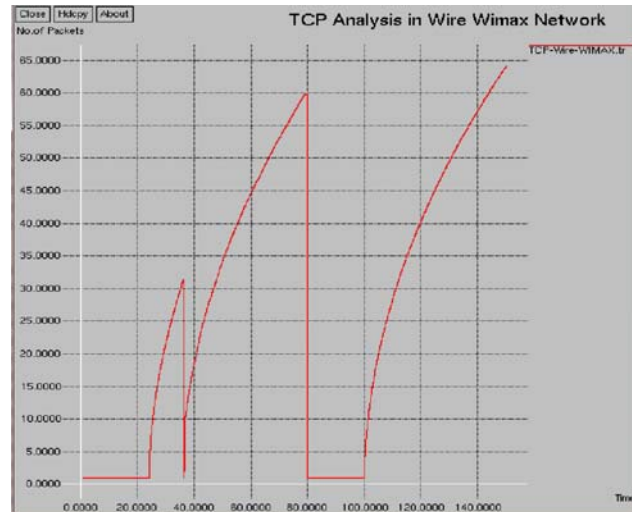


Figure 4 TCP Analysis in Wired-WIMAX network

### VIII. CONCLUSION AND FUTURE WORK

Theoretically Wired network support up to 11 Mbps data rate but in real world it has the data capability of 4 Mbps or little less than this. The most notable disadvantage of Wired is its range and WIMAX has a very robust and flexible air interface.

MN and WN are no problem to communication in own network but for communication in between FA is necessary. By comparing the performance of WIMAX and Wired technology Agent is really a superior interface in between both technologies. Results are clearly shows that the wired WIMAX communication is better than WIMAX. It will also resolve some of the technical difficulties of Cellular network. Moreover it is highly flexible and spectrally efficient. It is not far away where everybody will be able to access the high speed internet connectivity at any time at any place like the mobile phone we use today.

Performances of WIMAX-Wired hybrid network are better than the WIMAX, if here we consider single Agent. Now in future we also observe the performance of WIMAX in case of more than two Agents and also with heavy congestion and try to do work in image encryption and decryption in MANET with WIMAX Technology.

#### REFERENCES

- [1] Y. Tara et.al. "Policy-Based Threshold for Bandwidth Reservation in WIMAX and Wi-Fi Wireless Networks," En Proc. 2007 *Wireless and Mobile Communications. ICWMC '07. Third International Conference on*, pp.76.
- [2] E. M. Royer et.al. "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless" IEEE Persnal communication, 1999,pp. 46-55.
- [3] Johan Schiller. Mobile Communications. Addison-Wesley, 2001
- [4] WIMAX Forum. www.WIMAX.com/home -2007", McGraw-HILL 2005
- [5] Clint Smith et.al. "3G WIRELESS WITH WIMAX AND Wi-Fi 802.16 and 802.11, 2010..
- [6] Kejie Lu et.al. "WIMAX Networks: From Access to Service Platform", IEEE Network, Vol. 22, No. 6, May-June 2008, pp. 38-45.
- [7] Qiang Ni, "Performance Analysis and Enhancements for IEEE 802.11e Wireless Networks", IEEE Network, Vol. 19, No. 4, July-Aug. 2008, pp. 21-27.
- [8] T. Nissila, et.al. "WIMAX Backhaul for Environmental Monitoring", in Proc. Seventh International ACM Conference on Mobile and Ubiquitous Multimedia (MUM), Umea, Sweden, December 2008, pp. 185-188.
- [9] Kejie Lu et.al "A Secure and Service-Oriented Network Control Framework for WIMAX Networks", IEEE Commun. Mag., vol. 45, no. 5, pp. 124 – 130, May 2007.
- [10] S. R. Das et.al "Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks," in IEEE Personal Communication's Magazine special issue on Ad hoc Networking, pp. 16–28 (2010).
- [11] R. Bera et.al. "Wireless Embedded System for Multimedia Campus Network Utilizing IEEE 802.11 N (draft) and WIMAX Radio," en Proc. 2007 *Wireless and Optical Communications Networks*, pp.1-5.
- [12] S. Jindal et.al. "Grouping WI-MAX, 3G and WI-FI for wireless broadband," en Proc. 2005 *First IEEE and IFIP International Conference in Central Asia*.
- [13] Charles E. Perkins et.al "Ad hoc On-Demand Distance Vector (AODV) Routing", draft-ietf-manet-aodv-11.txt, June 2002.
- [14] T. Su-En. "WIMAX-Prospect and New Business Models, " en Proc. 2005 *3G and Beyond, 2005 6th IEE International Conference on*, pp.1-5.
- [15] A.Maheswara Rao, S.Varadarajan and M.N.Giri Prasad "CROSS-LAYER BASED QoS ROUTING PROTOCOL ANALYSIS BASED ON NODES FOR 802.16 WIMAX NETWORKS", International Journal of Advances in Engineering & Technology, Sept 2011. IJAET ISSN: 2231-1963
- [16] Yogesh Chaba, Yudhvir Singh and Amit Kumar, "AODV with Source Route Accumulation for improved Routing in WiMAX", IJCSI

International Journal of Computer Science Issues, Special Issue, ICVCI-2011, Vol. 1, Issue 1, November 2011 ISSN (Online): 1694-0814.

- [17] S. Srikanth and P. A. Murugesu Pandian, "Orthogonal Frequency Division Multiple Access in WIMAX and LTE A Comparison", IEEE Communications Magazine, pp-151-161, September 2012.
- [18] Mohd Nazri Ismail et.al. "A Simulation Model Design and Evaluation for AggregateTraffic Over Local Area Networks", International Journal of Advanced Computer Engineering,2009.
- [19] Saeed A. Bawazir et.al. "Performance of Infrastructure Mode Wireless LAN Access Network Based on OPNETTM Simulator", 2006.
- [20] Fast NS-2 simulator w <http://lst.inf.ethz.ch/fast-ns2/>

#### Author Profile



I am Kalyani Chaturvedi, M.Tech Final Year Student in T.I.E.I.T. Bhopal affiliated with R.G.P.V. University. My research topic is MANET (Mobile Ad.hoc Network) by that I try to done my dissertation in MANET in MAC lay. I have done my B.E. in Bansal College of Engineering, Manideep Bhopal in 2010.

# Augmented Reality in ICT for Minimum Knowledge Loss

Mr. RamKumar  
Lakshminarayanan  
Department of IT,  
HCT,  
Muscat, Oman.

Dr. RD.Balaji  
Department of IT,  
HCT,  
Muscat, Oman

Dr. Binod kumar  
Department of IT,  
HCT,  
Muscat, Oman

Ms. Malathi Balaji  
Department of IT,  
HCT,  
Muscat, Oman

**Abstract**—Informatics world digitizes the human beings, with the contribution made by all the industrial people. In the recent survey it is proved that people are not accustomed or they are not able to access the electronic devices to its extreme usage. Also people are more dependent to the technologies and their day-to-day activities are ruled by the same. In this paper we discuss on one of the advanced technology which will soon rule the world and make the people are more creative and at the same time hassle-free. This concept is introduced as 6<sup>th</sup> sense technology by an IIT, Mumbai student who is presently Ph.D., scholar in MIT, USA. Similar to this research there is one more research going on under the title Augmented Reality. This research makes a new association with the real world to digital world and allows us to share and manipulate the information directly with our mental thoughts. A college which implements state of the art technology for teaching and learning, Higher College of Technology, Muscat, (HCT) tries to identify the opportunities and limitations of implementing this augmented reality for teaching and learning. The research team of HCT, here, tries to give two scenarios in which augmented reality can fit in. Since this research is in the conceptual level we are trying to illustrate the history of this technology and how it can be adopted in the teaching environment.

**Keywords:** *Augmented Reality, 6<sup>th</sup> sense technology, Teaching and Learning, ICT*

## I. INTRODUCTION

Augmented Reality is a live, direct and indirect, view of a physical, real-world environment where the information about the surrounding real world of the user becomes interactive and digitally modified. [1]

Augmented Reality (AR) is taking digital or computer generated information, whether let it be images, audios, videos and touch or haptic sensations and overlaying them over in a real-time environment [2].

### A. Characteristics of Augmented Reality

The three characteristics of augmented reality are as follows:

- AR combines real and virtual information.
- AR is interactive in real time.
- AR operates and is used in a 3D environment.

## II. HISTORY OF AUGMENTED REALITY

In 1962, Morton Heilig, designed a multi-sensory technology that had visuals, sound, vibration and smell. It is a motorcycle simulator Sensorama.

A device paired to a headset such as harness or helmet is called head-mounted display (HMD). In 1968, Ivan Sutherland created an optical see-through HMD and one of the examples used six degrees-of-freedom. He called it as Sword of Damocles.

In 1975, Myron Krueger created Videoplace, which allowed users to interact with virtual objects. In 1992, Tom Caudell and David Mizell coined the term "Augmented Reality" at Boeing's Computer Services' Adaptive Neural Systems Research and Development project.

Markers are physical objects or places where the real and Virtual Environment are fused together. The idea of 2D matrix marker was developed by Jun Rekimoto in the year 1996. D' Fusion was created a product for Augmented Reality. 3D markers were presented by Mathias Mohring in Mobile phones in the year 2004. In the year 2006, Nokia initiated the image captured by the camera and annotated the users surrounding in real time with graphics and text. Wikitude World Browser which combines the GPS and compass data with Wikipedia entries which overlays the information with smartphone camera was launched in the year 2008.

## III. AUGMENTED REALITY DEVICES

The main devices for Augmented Reality are displays, input devices, tracking and computers. The types of displays are head mounted displays (HMD), handheld displays and spatial displays. The types of input devices for AR systems are gloves, wireless wristband, smart phones with touch screen. The types of tracking devices are digital cameras, optical sensors, GPS, accelerometers, solid state compasses, wireless sensors etc., Earlier computers was used to process the camera images, but now with the advent of the smartphone technology the usage of computers as back pack configuration is considerably reducing.

## IV. AUGMENTED REALITY INTERFACE

The interaction in AR applications is classified as tangible AR interfaces, collaborative AR interfaces, hybrid AR interfaces, and the emerging multimodal interfaces.

Direct interaction with the real world by exploiting the use of real, physical objects and tools is supported by Tangible interfaces. For the use of multiple displays to support remote and co-located activities collaborative AR interfaces are used. Hybrid interfaces combine an assortment of different, but complementary interfaces as well as the possibility to interact through a wide range of



interaction devices. Multimodal AR Interfaces combine real objects input with naturally occurring forms of language and behaviors such as speech, touch, natural hand gestures, or gaze.

## V. AUGMENTED REALITY SYSTEMS

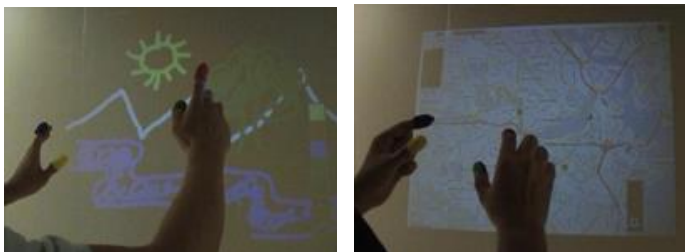
Fixed indoor systems, fixed outdoor systems, mobile indoor systems, mobile outdoor systems and mobile indoor and outdoor systems are the five categories of Augmented Reality Systems.

## VI. AUGMENTED REALITY MOBILE SYSTEMS

Augmented Reality Mobile Systems includes both the mobile phone applications and the wireless systems.

## VII. SIXTHSENSE / WUW - WEAR UR WORLD

*'SixthSense' is a wearable gestural interface that augments the physical world around us with digital information and lets us use natural hand gestures to interact with that information. By using a camera and a tiny projector mounted in a pendant like wearable device, 'SixthSense' sees what you see and visually augments any surfaces or objects we are interacting with. It projects information onto surfaces, walls, and physical objects around us, and lets us interact with the projected information through natural hand gestures, arm movements, or our interaction with the object itself. 'SixthSense' attempts to free information from its confines by seamlessly integrating it with reality, and thus making the entire world your computer. [4]*



## VIII. OPTICAL CHARACTER RECOGNITION

Optical Character Recognition (OCR) is the mechanical or electronic translation of scanned images of handwritten, typewritten, or printed text, to machine encoded text. OCR is mainly used in language translation, digital libraries and even in the postal services. Now a day's most of the mobile phones are having high end camera functionality and means of enabling the features of OCR in mobile.

## IX. QR CODE

QR Code abbreviated from Quick Response Code was invented by Denso Wave, Japan. QR Code can detect the 2 Dimensional digital images. QR Code Reader can be a

mobile phone to capture the dimensional images. The reader locates the three distinctive squares at the corners of the image, and uses a smaller square near the fourth corner to normalize the image for size, orientation and angle of viewing. The small dots are converted to binary numbers and their validity checked with an error-correcting code. QR Codes can be used with most of the mobile operating systems.

## X. SCENARIO 1

HCT is having 14,000 students studying in 8 departments in 8 buildings. Each department is having around 100 academicians and 20 other administrative staff. In administrative building there is more than 50 administrative staff members are working. Within each department there are at least 5 to 10 specializations are offered. Students and academicians are divided by their specialization. Again in each specialization students and staff are divided by levels like Diploma, Advanced Diploma and B.Tech., Every student is assigned with an advisor for allocating subject for the Academic semesters. Each course there will be a course coordinator and course teacher. Apart from that each student may take help from the administrative people of the department for their smooth progress in their studies. Many a times HCT is receiving complaints from students that they are facing problem in identifying the solution for solving some issues with a particular staff. Since staff members are in different staff room and cabin, it is difficult for a student to check where the particular staff seated or not. Similarly academic staff also complains that most of the time they spend in informing the students where a teacher is seated and the location of the building.

At this stage, we felt Augmented Reality can be applied to overcome the above problem particularly during the period of examination and time table registration of HCT. A student downloads the **HCT Identify Staff** app from the HCT website's mobile application page. By means of selecting student ID, student will be listed down his Advisory Name. The staff list, their specialization and QR Code with position information is available in the entrance board. The student will scan a QR code from the entrance board to find his staffs desks. This scenario highlights the potential of using QR codes for indoor AR navigation systems. Installation of a QR code is very low cost and easy to implement. Such codes can be installed in places where staffs change location so as to identify the staff's current location, while the student moves towards the staff desk he will be given direction by voice to match he reached the staff's location, it will be provided in AR view. AR view would be very intuitive so as to reduce navigation error and the time required for a student to understand the navigation information he is being informed.

## XI. SCENARIO 2

Any Technology will be successful only when it tempts or impresses a person to use it. Both in academic environment and administrative environment, this technology will give great impact when it is practiced for

teaching and learning process. During the discussion with the research team, everyone felt that new technology should not be tried with the beginners as well as people at the exit level. Hence we have decided to take sample from the Advanced Diploma Level.

In the recent survey we have found students are facing problem in learning practical subjects like SQL concepts and Syntax. Here it is more difficult for the students to remember lot of syntax and commands. The research team decided to create Augmented Reality application which will automatically produce the SQL syntax when it scans data which needs to be stored in the database. For example: When a student scans a table structure as input with the mobile phone, the application should generate the corresponding SQL code as output. A sample of the table structure and SQL Code are given below:

A. *Proposed Table Structure:*

**Student\_Mark**

Column Name	Data type	Size	Constraint
Stud_id	Number	9	Primary key
Stud_Name	Varchar2	25	
Prog_id	Varchar2	10	Unique
Course_id	Varchar2	8	
Quiz1	Number	5,3	
Mid Exam	Number	5,3	
Final	Number	5,3	
Total	Number	6,3	Check <100
Grade	Varchar2	2	
Result	Varchar2	10	Check "pass" or "fail"

B. *Expected Code:*

```
Create table Student_Mark (  
Stud_id number(9) primary key,  
Stud_Name Varchar2(25),  
Prog_id Varchar2(10) Unique,  
Course_id Varchar2(8),  
Quiz1 Number(5,3),  
Mid_Exam Number(5,3),  
Final Number(5,3),  
Total Number(6,3) constraint SMCH1 check total < 100,  
Grade Varchar2(2),  
Result Varchar2(10) check SMCH2 check (result = 'pass' or  
'fail'));
```

The proposed system will be using OCR capture technology. The text is printed on the paper with a specific format in the fixed height and width captured by OCR. The application will capture and rectify images will be fed in to the OCR Engine. This application will use the mobile device's camera to capture the images (like smart phone camera). Once the OCR process is over, the syntax engine

will collect the information from the process image and create the SQL query.

## XII. CONCLUSION

This paper mainly concentrates on the Augmented Reality and the 6<sup>th</sup> sense technology due to the advantages of simplicity in this technology. This technology can be implemented in the near future with the minimum requirements of the resources, compared to the 6<sup>th</sup> sense technology. Still we felt it is not justified if we leave 6<sup>th</sup> sense technology without mentioning here. In the Augmented Reality we have mentioned the history, devices and interfaces. HCT Research reveals that 95% of the students are using their smart phones or mobile devices for their day-to-day learning process. HCT is also encouraging students to use E and M learning devices. The Augmented Reality device section gives confidence to us about the implementation of this technology. Most of the features required by the Augmented Reality are there with the smart phones in the recent days. The scenario's specified here are just a conceptual proposal by the research team of HCT, to successfully implement this new technology and to evaluate the improvements in the teaching and learning process. The next stage is to evaluate the knowledge loss in the learning process by this technology. It is obvious that any new technology may have some negative impacts in future that also to be evaluated after the implementation of this new technology.

## REFERENCES

- [1] Wikipedia.org accessed on Dec 30, 2012
- [2] Greg Kipper, Joseph Rampolla, Augmented Reality: An Emerging Technologies Guide to AR, Elsevier, Dec 27, 2012
- [3] Borko Furht, Handbook of Augmented Reality, Springer, Jan 1, 2011
- [4] <http://www.pranavmistry.com/> accessed on Dec 31, 2012
- [5] Sonia Bhaskar et al., Implementing Optical Character Recognition on the Android Operating System for Business Cards, "EE 368 Digital Image Processing Notes" Spring 2010
- [6] B. Girod. "EE 368 Digital Image Processing Notes," EE 368 Digital Image Processing Spring 2010.
- [7] Gee Andrew et al., A topometric system for wide area augmented reality. Computers and Graphics 2011
- [8] P. Serrano-Alvarado, C. Roncancio and M. Adiba, "A Survey of Mobile Transactions," Distributed and Parallel Databases, September 2004
- [9] Fröhlich P, Oulasvirta A, Baldauf M, Nurminen A. "On the move, wirelessly connected to the world", Commun ACM 2011
- [10] Henrysson A, Ollila M, Billinghurst M. "Mobile phone based AR scene Assembly". In: Proc 4th Int Conf Mob Ubiquitous Multimedia - MUM '05, ACM Press; 2005
- [11] Reilly DF, Inkpen KM, Watters CR. "Getting the Picture: Examining How Feedback and Layout Impact Mobile Device Interaction with Maps on Physical Media", In: Int Symp Wearable Comput - ISWC '09, IEEE Press; 2009
- [12] Costabile M, Angeli AD, "Explore! possibilities and challenges of mobile learning", In: Proc 26th Annu Int Conf Hum Comput Syst. – CHI'08, ACM Press: 2008



- [13] <http://www.rummbble.com>
- [14] Spohrer J., Information in Places, IBM System Journal 38(4), 1999
- [15] Acquisti, A. and Gross, R., Imagined Communities : Awareness, Information Sharing and Privacy on the Facebook. PET 2006.
- [16] Gogging G., Cell Phone culture: Mobile technology in everyday life, Routledge, New York 2006.
- [17] Greene K., Hyperlinking reality via phones. MIT Technology Review 2006.
- [18] L. Bonanni, M. Seracini, X. Xiao, M. Hockenberry, B.C. Costanzo, A. Shum, R. Teil, A. Speranza and H. Ishii, International Journal of Creative Interfaces and Computer Graphics, 2010
- [19] D.M. Popovici, R. Querrec, C.M. Bogdan and N. Popovici, International Journal of Computers, Communications & Control, 2010
- [20] Langlotz Tobias, Degendorfer Claus, Mullone Alessandro, Schall Gerhard, Reitmayr Geehard, Schmalstieg Dieter, Robust Detection and tracking of annotations for outdoor augmented reality browsing, Computer and Graphics 2011.
- [21] Philbin J., Chum O., Isard M., Sivic J., and Zisserman A., Object retrieval with large vocabularies and fast spatial matching. In Proc of CVPR, 2007.
- [22] Phibin J., Chum O., Isard M., Sivic J., and Zisserman A., Lost in quantization: Improving particular object retrieval in large scale image databases. In Proc of CVPR, 2008.
- [23] Swan J.E and Gabbard J.L., Survey of User-Based Experimentation in Augmented Reality, presented at Ist International Conference on Virtual Reality, Las Vegas, Nevada, 2005.
- [24] Sivic J and Zisserman A., Video google: A text retrieval approach to object matching in videos. In Proc of ICCV, 2003.
- [25] Wagner D., Langlotz T. and Schmalstieg D., Robust and Unobstructive marker tracking on mobile phones. In Proc. Of ISMAR'08, 2008.

#### AUTHORS PROFILE

**Ramkumar Lakshminarayan:** He is post graduate in Computer Science and at present working as a Lecturer, Computer Science in Higher College of Technology, Muscat. He is having 14 years of experience in teaching, consulting and software development. He has conducted training for leading corporate companies in India and abroad in the field of Database, Datawarehousing, Cloud Computing and Mobile Technology. He has presented articles in various journals around the Globe. He has did research in the field of Applications of Computers Science in the Management of AAVIN Dairy Cooperatives and submitted thesis to Bharathidasan University, India. He has conducted workshop in events of Free and Open Source Software.

**Malathi Balaji:** She did her Master of Computer Science from Anna University with Gold medal. Having rich experience in teaching at graduate and post graduate level

for more than 8 years. Presently waiting for Ph.D., registration with reputed university. She has published many papers in national and international journals during her studies. She has proved her excellence in education from her childhood by scoring district ranking in 10<sup>th</sup> and 12<sup>th</sup>, as well as distinction in her UG. Presently doing research in Networks field and certified by CISCO. She has worked in abroad also as corporate trainer.

**Dr. RD.Balaji:** He has completed his Ph.D., in the year 2010 in Computer Science. Preceding to this Ph.D., completed his Bachelors and Masters degree from Madurai Kamaraj University. He is having totally fifteen years of teaching at UG and PG level including ten years of abroad experience. Presently working in Higher College of Technology, one of the prestigious Colleges in the Sultanate of Oman. Published many papers in national and international Journals. He has visited more than 8 countries to present his research work. He has guided many M.Phil., students to do their research. He is in the process of getting guideship from universities. He evaluated many Ph.D., thesis as a foreign examiner. Having membership with more than ten international computer oriented institutions and member of editorial board and reviewer for many journals and conferences.

# Optimizing Cost, Delay, Packet Loss and Network Load in AODV Routing Protocol

Ashutosh Lanjewar  
M.Tech (DC) Student  
T.I.E.I.T. (TRUBA)  
Bhopal (M.P), India

---

Neelesh Gupta  
Department of Electronics & Communication  
T.I.E.I.T. (TRUBA)  
Bhopal (M.P), India

---

**Abstract:** AODV is Ad-hoc On-Demand Distance Vector. A mobile ad-hoc network is a self-configuring network of mobile devices connected by wireless. MANET does not have any fixed infrastructure. The device in a MANET is free to move in any direction and will form the connection as per the requirement of the network. Due to changing topology maintenance of factors like Packet loss, End to End Delay, Number of hops, delivery ratio and controlling the network load is of great challenge. This paper mainly concentrates on reducing the factors such as cost, End-to-End Delay, Network Load and Packet loss in AODV routing protocol. The NS-2 is used for the simulation purpose.

**Keywords:** AODV, Power consumption, End-to-End Delay, Network Load

## I. INTRODUCTION

Mobile Ad-Hoc network mainly concentrates on wireless communication without any fixed infrastructure. Wireless communication has wide application in Security zones. In past there is only a fixed wireless communication network exists where communication range is bonded. Now there advanced Ad-Hoc network and Mobile Ad-Hoc network are introduced where all nodes share data among themselves. The nodes in AODV may connect and leave the network at any time [10]. All Ad-Hoc routing protocol have different routing strategies so factors such as End to End Delay, Traffic Overhead and packet delivery ratio and power consumption gets vary. Routing mainly deals with the route discovery between the source and destination [4]. Nodes in network change the position as per requirement of system so topology varies time to time. The routing Protocols are mainly divided in to Routing and Reactive Protocol. Proactive routing protocols (e.g.OLSR) are table-driven. Link-state algorithms maintain a full or partial copy of the network topology and costs for all known links. The reactive routing protocols (e.g. AODV) create and maintain routes only if these are needed, on

demand. They usually use distance-vector routing algorithms that keep only information about next hops to adjacent neighbors and costs for paths to all known destinations. Thus, link-state routing algorithms are more reliable, less bandwidth-intensive, but also more complex and compute and memory-intensive. AODV routing protocol is a reactive routing protocol. AODV is a related to the Bellman-Ford distant vector algorithm. In AODV a route to a destination is determined when a node wants to send a packet to that destination. Routes are maintained as long as they are needed by the source. When the packet is transmitted from source to destination there are many nodes involved between the successful receptions of packets. ADOV routing protocol uses RouteRequest (RREQ) RouteReply (RREP) and RouteError (RERR) as a control signal. When a source node desires to send a message to some destination node and does not have a valid route to that destination it looks for a Path to locate the other node. Source node sends a RREQ packet to its neighbors, which then forward the request to their neighbors, and the process go on until route to the destination is located [2]. During the process of forwarding the RREQ, the entry of intermediate nodes get record in to their routing tables which include the address of the neighbors from which the first copy of the broadcast packet is received. This will help to find a path. If in case some additional copies of the same RREQ are received later than these packets are discarded. Once the RREQ reaches the destination node, the destination or intermediate node responds by sending a RREP packet back to the neighbor from which it first received the RREQ. When packet transmission is in progress various factors play measure role. It is observed that packet may get drop in between due to bad linkage quality and lack of proper communication channel between the nodes. Sometimes communication gets successful but the backend factors such as End to End delay, Power consumption, Routing overhead and hop limit really makes the network really costly and unreliable one. In AODV the routing

table plays the important role. The route table includes the entry at each node with the information regarding the sequence number for IP address of destination node. The RREQ, RREP and RERR commands are received by node utilized for the updating of the sequence number. The destination node can increment its sequence number when there is time for source node to start a route search or when there is time for destination node to generate the RREP message against the RREQ response of source node. In routing table the route gets updated with new sequence numbers when it is higher than the destination sequence numbers. There are other two possibilities, the first one is when the new sequence number and destination sequence numbers are equal but if sum number of hop plus one additional one hop in new sequence routing table is smaller than hop count in the existing destination sequence number and secondly when the existing sequence number is unknown.

The rest of this paper is ordered as follows. The related works are discussed in Section II, Section III represents working of AODV routing protocol and Section IV gives idea regarding the proposed work. Section V gives detail of simulation results and its discussion. Section VI provides conclusion and future work whereas section VII represents References.

## II. RELATED WORK

AODV is reactive routing protocol. It is simple, efficient and effective routing protocol having wide application [14]. The topology of the network in AODV gets change time to time so dealing with same and as well as maintaining the Cost, End-to-End, Network Load and Packet Loss is great challenge. Various researches have been carried out on above factors. Lalet.al. [13] implemented new NDMP-AODV that is able to provide low end-to-end delay and high packet delivery ratio, while keeping low routing overhead. In future work they improve the route selection process of NDMP-AODV so that it can select routes that can satisfy user application requirements. Raj Kumar G.et.al [15] evaluated the AODV and DSR on parameter such as Throughput, Delay, Network Load and Packets Drop against pause time. They observed that AODV performs well in the presence of noise gives better throughput level with less delay, consumes less energy and less packets get drop. Mauryalet.al. [2] Compared on-demand routing protocols that is reactive and proactive routing. They observed that reactive protocol offers quick adaptation to mobile networks with low processing and low bandwidth utilization. In [3] Das et.al. two on-demand routing protocols, DSR and AODV had been compared. In future, they have studied more routing protocols such as DSDV, TORA based on parameters such as fraction of packet delivery, end to end delay and routing overhead. Yanget.al. [5] compared the AODV, R-AODV and SR-AODV. From simulation they have concluded that SR-AODV improves the performance of AODV in most metrics, as the packet delivery ratio, end to end delay, and Power consumption. Yanget.al.[7] analyzed the performances of

AODV and M-AODV they observed that in M-AODV route discovery succeeds in fewer tries than AODV. When the simulation is carried out they conclude that M-AODV improves the performance of AODV in most metrics, as the packet delivery ratio, end to end delay, and energy consumption. Li et.al. [6] evaluated the TRP with S-AODV and it is observed that TRP improves network performance in terms of energy efficiency and average routing delay. In [4] Thanthyret.al. they verified the EMAODV with the AODV. The results obtained from the simulations show that EMAODV performs better than AODV in terms of throughput, number of route discoveries, control overhead and packet drops but, the average end-to-end delay of EM-AODV was found to be higher than AODV. Khelifaet.al.[1] investigated the performances of M-AODV and AODV they observed route discovery succeeds in that M-AODV improves the performance of AODV in terms of metrics, packet delivery ratio, end to end delay, and energy consumption. In future they studied the implementation of Energy AODV mechanism to conserve more energy. Sharma et al.[8] evaluated the effect of different scheduling algorithms for AODV and modified AODV. They reduce the average delay between the nodes communication. Wei et.al [9] worked on Demand Distance Vector (IPODV) routing protocol considering the topological feature of the power-line network. In future they work on the routing maintenance mechanism and the neighbor table management of the AODV routing Protocol. Chaurasia et.al. examined[11] on OLSR, DSDV, DSR, AODV, and TORA protocols. They observed that due to the infrastructure less structure of protocol security and power awareness is difficult to achieve in mobile ad hoc networks. In future they work on core issues of security and power consumption in these routing protocol. M.Ushaet.al. [12] implemented new advanced AODV name RE-AODV (Route-Enhanced AODV). They observed routing overhead is reduced by 25% and end to end delay of packets 11% as compared to normal AODV protocol. It has been observed in AODV routing protocol that power consumption is more which make AODV a costly one. The end-to-end delay is more, there increase the chances for loss of information while transaction between the source node and destination node. So the effort are required to be taken regarding the reduction of power consumption and end-to-end delay in order to reduce the costing in implementation of AODV routing protocol.

The related work in the field of AODV routing protocol really creates the motivating impact on the mind for further research. The implementation of the AODV routing protocol with all features such as less end-to-end delay, maintenance of network Load, Packet loss and cost is really a challenging one. The proposed work mainly concentrates on implementation of all above parameters. This implementation will really prove advantageous for the networking technology.

## III. AODV ROUTING PROTOCOL

AODV is a self-starting and dynamic algorithm where the large number of nodes can participate for establishing communication and maintaining AODV network. The topology of AODV changes time to time as the nodes are not fixed to any standard position. In AODV hello messages are used to detect and monitor links between the nodes. An active node periodically broadcasts a Hello message to all its neighboring nodes. If in case the nodes fail to transmit hello message to neighboring node, the complete network will collapse due to link breakage. AODV uses mainly three message types Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RERRs). These messages are carried through UDP and IP headers. When the source node wants to send data to the destination node it sends the RREQ message. This RREQ message may be received directly by the destination node or intermediate node. In AODV the destination sequence number is generated. During the period when the node requests for the route discovery it is provided with destination sequence numbers. A requesting node is required to select the one with the greatest sequence number. Then the route is made available by unicasting a RREP back to the source node from where the RREQ is sent. AODV mainly deals with route tables. In route tables the information of all the transactions between the nodes are kept. The routing request has following sections: Source address, Request ID, Source sequence number, destination address, destination sequence number and hop count. The route request ID gets incremented during single transaction from source node. At the destination node the Request ID and source address are verified. The route request with same request ID is discarded and no route reply message will generate. Every route request has its TTL i.e. Time To Live and during this time period the route request can be retransmitted if reply is not received from destination node. If the route is valid then destination node unicasts the route reply message to the source node. The route Reply has following sections: source address, destination address, destination sequence number, hop count and life time. Hop count defines number of nodes utilized for data. When node involved in active transaction gets lost, a route error (RERR). The message format of route request, route reply and route error are given below.

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
Type										J	R	G	L	U	Reserved										Hop Count														
RREQ ID																																							
Destination IP Address																																							
Destination Sequence Number																																							
Originator IP Address																																							
Originator Sequence Number																																							

**Figure 1. Message Format of (RERQ)**

In figure 1 Type of RREQ is 1. J represents the Join flag and R represents Repair flag both are reserved for multicasting purpose. G represents Gratuitous RREP flag

which indicate that data is unicast to the node with specified Destination IP address field. D represents that only destination will respond to the RREQ and no intermediate node will act. U represents that sequence Number is unknown.

0										1										2										3																			
0123456789012345678901234567890123456789012																																																	
Type										RA		Reserved										Prefix size										Hop Count																	
Destination IP Address																																																	
Destination Sequence Number																																																	
Originator IP Address																																																	
Lifetime																																																	

**Figure 2. Message Format of (RREP)**

In figure 2 Type of RREP is 2. R represents Repair flag and it is used for multicast. A represents Acknowledgment required and Reserved is indicated by 1 when network is ready to give route reply or by 0 then no reply will be given to route request. Prefix size represents that next hop may be used for any nodes with the same routing prefix.

Now in figure 1 and figure 2 Hop count represents the number of hops required during the retransmissions. Destination IP Address represents IP address of destination to which route is to be generated. Destination Sequence Number is always related with the route. Originator IP Address represents the source from which the RREQ is generated whereas; the Life time is the time period during which the node receives the RREP to validate the route.

0										1										2										3																			
0123456789012345678901234567890123456789012																																																	
Type										N	Reserved																				Destination Count																		
Unreachable Destination IP Address																																																	
Unreachable Destination Sequence Number																																																	
Additional Unreachable Destination IP Address(If Needed)																																																	
Additional Unreachable Destination Sequence Number (If Needed)																																																	

**Figure 3. Message Format of (RRER)**

In figure 3 Type of RRER is 3. N represents that flag will not get delete. Reserved is sent as 0 represents that RERR is ignored. Destination Count represents the number of destinations that are out of reach and this count will included in the message. Unreachable Destination IP Address represents the IP address of destination is not reachable due problem in link whereas Unreachable Destination Sequence Number represents sequence number of destination whose IP address is not reachable due to link breakage.

## VI. PROPOSED METHOD

The performance comparison of Normal AODV and newly generated AODV routing protocols are analyzed and tested for 40 nodes when simulations are carried on NS-2 simulator. The AODV routing protocol will perform better than past ones. The cost and end-to-end delay will get reduce also there by minimize the network load and packet loss. Special concentration is given on controlling the hop limit. The number of nodes utilized for single transaction from assigned source to destination will get reduced. As hop limit is achieved indirectly it affects network load, end-to-end delay and indirectly the probability of packet loss. The ultimate cost of the network gets reduce in AODV routing protocol. In the project the Euclidean distance between the nodes is calculated which gives the idea regarding time require to transfer data from source to destination and distance between the source and destination. Thus the Euclidean distance formula is used for determining the costing of the network. The AODV network with nodes P, Q, R, S, and T is given in figure 4. Consider the two dimension Euclidean space.

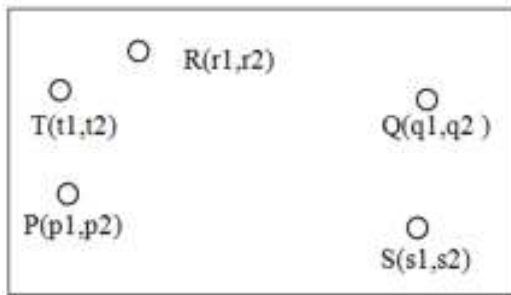


Figure 4. Nodes in two dimension Euclidean space

. In order to find the Euclidean distance between two nodes P and Q, first of all P and Q are described with coordinates  $(p1, p2)$  and  $(q1, q2)$  respectively. In first step length between the P and Q is given by  $|p1 - q1|$  and  $|p2 - q2|$ . Secondly the Pythagorean Theorem is between the two length gives  $((p1 - q1)^2 + (p2 - q2)^2)^{1/2}$ . So the distance between two points  $P = (p1, p2)$  and  $Q = (q1, q2)$  in two dimensional space is there given as  $=$

$\sqrt{(p1 - q1)^2 + (p2 - q2)^2}$ . Similarly the distance between two points  $P = (p1, p2, \dots, pn)$  and  $Q = (q1, q2, \dots, qn)$  in n dimensions Euclidean space can be given as

$$\sqrt{(p1 - q1)^2 + (p2 - q2)^2 + \dots + (pn - qn)^2}$$

The key advantages of the proposed work are multiple. The good network mainly concerns with the efficient transfer of data, minimum costing, less packet loss and Network Load. The performance of Normal AODV and AODV routing protocols are compared based on the performance metrics which are given below. The four parameter are evaluated against number of transfers.

**Cost:** It depends on number of nodes utilized, power consumed and packet loss.

**End to End delay:** It is the difference between the packets received time and packet sent time.

**Packets drop:** It is the number of packets lost in transit.

**Network Load:** The total traffic (bits/sec) received by the network layer from the higher MAC that is accepted and queued for transmission.

## V. SIMULATION RESULTS AND DISCUSSION

The simulation has been done for 40 nodes using Network Simulator 2.35 in an area of size 1000 m x 1000m. The performance metrics such as cost, end to end delay and Network Load are evaluated against number of transfers for both Normal AODV and New advance AODV Routing protocols and are shown below. The red colour curve represents the Normal AODV protocol while the green colour curve represents the proposed new advance AODV protocol. The Simulation Parameters are given below

Number of Nodes	40
Routing Protocol	AODV
Traffic Source	CBR
Area	1000 m x 1000 m
Mac Type	IEEE 802.11
Tool	NS-2.35

Table I –Simulation Parameters

In Figure 5. Number of Data transfers is plotted against the cost. In the graph only three data transfers are consider. It is observed that cost require in a new advance AODV routing is very less as compare with normal AODV. Cost in Proposed AODV simulation touches the lower level of 153 units.

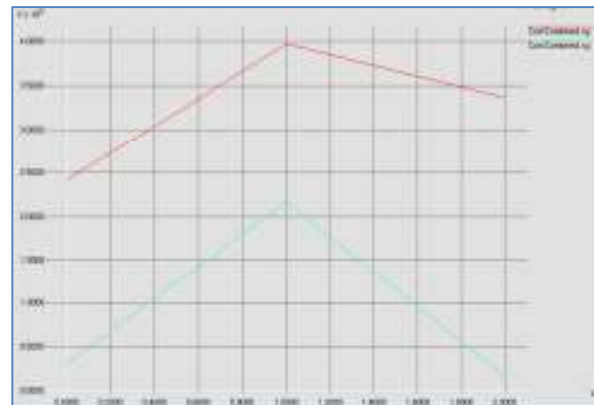


Figure 5. Number of Data Transfers versus Cost

In figure .6 the Number of data transfers is plotted against delay. It is observed from graph that Proposed AODV has

lowest delay in all data transfers as compare to normal AODV routing protocol.

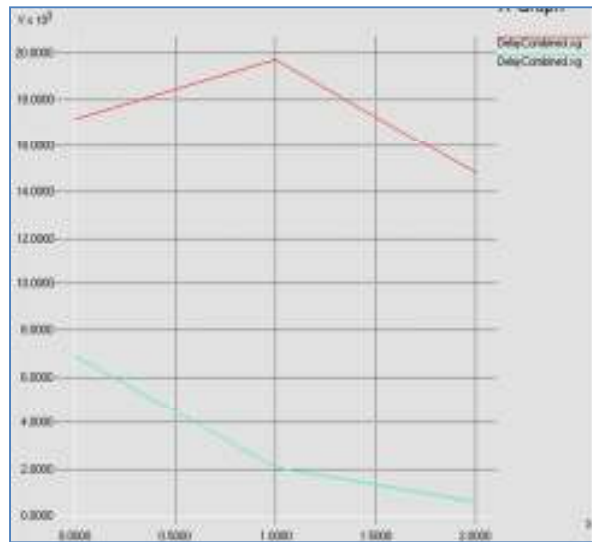


Figure 6. Number of Data Transfers versus Delay (ms)

In figure 7. The Number of data transfers is plotted against Packet loss. It is observed from graph that Proposed AODV has low packet loss as compare with normal AODV routing Protocol.

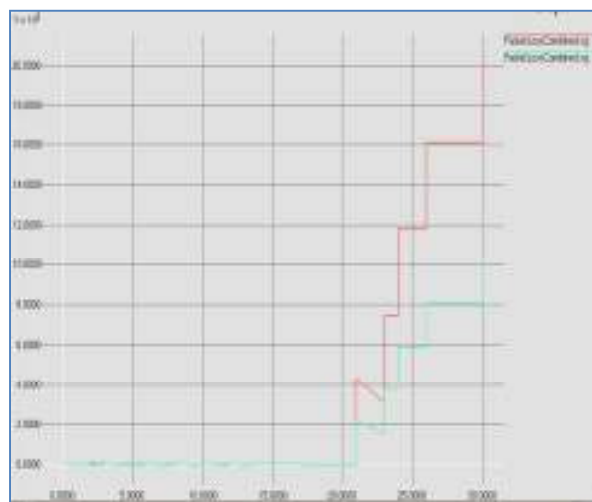


Figure 7. Number of Data Transfers versus Packet Loss

In figure 8 the Number of data transfers is plotted against Network Load. It is observed from graph that Proposed AODV has negligible network load in all data transfers as compare to normal AODV routing protocol.



Figure8.Number of Data Transfers versus Network Load

## VI. CONCLUSION AND FUTURE WORK

The performance metrics such as Cost, Delay, Network Load and Packets Drop are evaluated against Number of transfers for both Normal AODV and new advance AODV with number of mobile nodes of up to 40 using NS-2.35. As the number of nodes is increased, still new advance AODV performs well and yields better throughput level with less delay and consumes less energy. Despite having high Network load new advance AODV is able achieve less packets Drop when compared to Normal AODV protocol. In this simulation new AODV has the all-round performance.

## V. REFERENCES

- [1]Khelifa S., Maaza Z.M., "An Energy Multi-path AODV Routing Protocol in Ad Hoc Mobile Networks" IEEE International Symposium on Communications and Mobile Network , 2010 Conference Publications, pp.1-4, 2010.
- [2]Maurya P.K., Sharma G., Sahu V., Roberts A. and Srivastava M., "An overview of AODV Routing Protocol" International Journal of Modern Engineering Research (IJMER), Vol.2, Issue3, pp.728-732, 2012.
- [3] Das S.R., Perkins C.E., Royer E.M., "Performance Comparison of Two on-demand Routing Protocols for Ad-Hoc Networks", 19th annual joint conference of the IEEE Computer and communication Societies, IEEE Procc., pp.3-12, Vol.-1, Isreal, INFOCOM, 2000.
- [4]Thanthry N, Kaki S. R., Pendse R., "EM-AODV: metric based enhancement to aodv routing protocol", IEEE 64th Vehicular Technology Conference, pp.1-5, 2006.



[5]Yang H. , Li Z., “A Stability Routing Protocols base on Reverse AODV”, IEEE International Conference on Computer Science and Network Technology, Vol.4, pp.2419-2423, 2011.

[6]Li L., Chigan C., “Token Routing: A Power Efficient Method for Securing AODV Routing Protocol”, IEEE International Conference on Networking, Sensing and Control, pp.29-34, 2006.

[7]Yang H., Li Z., “Simulation and Analysis of a Modified AODV Routing Protocols”, IEEE International Conference on Computer Science and Network Technology, Vol.3, pp.1440-1444, 2011.

[8]Sharma D.K., Kumar C., Jain S., Tyagi N., “An Enhancement of AODV Routing Protocol for Wireless AdHoc Networks”, IEEE International conference on Recent Advances in Information Technology , pp-290-294, 2012.

[9]Wei G., Jin W., Li H., “An Improved Routing Protocol for Power-line Network based on AODV” IEEE International Conference on Communications and Information Technologies, pp.233-237, 2011.

[10]Gupta N, Gupta R., “Routing Protocols in Mobile Ad-Hoc Networks: an Overview”, IEEE International Conference on Emerging Trends in Robotics and Communication, pp.173-177, 2010.

[11]Chaurasia N., Sharma S.,Soni D., “Review Study of Routing Protocols and Versatile challenges of MANET”IJCTEEVolume2, Issue 1, pp.150-157, 2012.

[12] M.Usha, S.Jayabharathi, Banu R.S., “RE-AODV: An Enhanced Routing Algorithm for QoS Support in Wireless Ad-Hoc Sensor Networks” IEEE International conference on Recent Trends in Information Technology, pp.567-571, 2011.

[13]Lal C., Laxmi V. and Gaur M.S., “A Node-Disjoint Multipath Routing Method based on AODV protocol for MANETs”, IEEE 26th International Conference on Advanced Information Networking and Applications (AINA), pp.399-405, 2012.

[14]Perkins C.E, Royer E., “Ad-Hoc On-Demand Distance Vector Routing”, IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, 1999.

[15]Rajkumar G., Kasiram R. and Parthiban D “Optimizing Throughput with Reduction in Power Consumption and Performance Comparison of DSR and AODV Routing Protocols”, International Conference on Computing, Electronics and Electrical Technologies, pp.943-947, 2012.

## AUTHORS PROFILE



Ashutosh Lanjewar is Pursuing M.Tech in Digital Communication from Truba Institute of Engineering and Information Technology (T.I.E.I.T.), Rajiv Gandhi Proudhyogiki Vishwavidyalaya (RGPV), Bhopal (M.P.) - India. He has completed his B.E. in Electronics and Telecommunication in 2007 from

G.H.Raisoni College of Engineering, Nagpur (Maharashtra) - India. His area of research Interest is Wireless Communication and Networking.



Neelesh Gupta is Pursuing Ph.D in Electronics and Communication from Rajiv Gandhi Technical University (RGTU), Bhopal (M.P.)-India. He has a rich experience of teaching in various Technical institutions of reputed in MP-India. He is having more than 10 years of teaching Experience.

Presently he is an Assistant Professor in Truba Institute of Engineering and Information Technology (T.I.E.I.T.), Bhopal (M.P.) - India. He has earned his M.Tech degree in Microwave and Millimeter Wave in 2007 from MANIT, Bhopal. His area of research Interests are Wireless Communication, Microwaves and Digital Signal Processing. He has presented a number of research papers in various National, International conferences and reputed International Journals. He is Life time member of IETE, New Delhi.

## Data Structures and Internet Application Identification

Mrs. Mrudul Dixit  
Assistant Professor

Department of Electronics and Telecommunications  
Cummins College of Engineering for Women  
Karvenager, Pune – 411052, M.S. India.

Dr. Balaji V. Barbadekar  
Principal

Dyanganga College of Engineering, Pune,  
Maharashtra, India

**Abstract**— Internet traffic describes the number of packets of various applications moving on the network. The internet traffic is increasing enormously day by day and so there is a need to monitor the network and the traffic for network management and planning, traffic modeling and detection, bandwidth analysis, etc. The identification of internet applications can be done on the basis of well known port numbers. The identification of application leads to analysis of bandwidth utilization by various internet applications. The port numbers are stored using different data structures. When a packet is received the port number from the packet is matched with the port numbers in the data structures. The time required to map is analyzed and should be minimum. The space required to store the database also should be minimum. There is always a tradeoff between the space and time. This paper deals with the analysis of space and time requirements for identification of internet applications based on well known port numbers using the data structures Binary Search Tree, AVL tree and Skip list. The packet capturing is done using tcpdump and Libpcap library on Linux platform using 'C' Language.

**Keywords**- Internet traffic, port number, skip list, AVL tree, BST.

### I. INTRODUCTION

Network traffic monitoring is a very important and a necessary part of today's internet. Internet traffic tells about how many users are accessing the particular websites and from which location. The complexity of traffic increases giving rise to need for network monitoring. The traffic monitoring is required for different reasons such as internet packet / traffic identification for bandwidth analysis, planning and management of the networks, traffic modeling, etc. The traffic identification is done on the basis of the port number present in the packet. Port number is of 16 bits. Port numbers from 0 – 1023 are well known port numbers, 1024 to 49151 are registered ports and 49152 to 65535 are dynamic port numbers. Some port numbers above 1023 are also accepted as official port numbers by IANA. Table 1 lists the few internet applications, their protocols and the port numbers.

These well known port numbers are stored using the data structure and are searched to match the unknown port number from the captured internet packet. The analysis of space required for data structure and 'C' language program and time required to search are the trade offs. Various data structures such as array, link list, skip list, binary search tree etc. can be used for storing port numbers. The search

algorithms such as linear search, binary search, etc. can be used for matching the port number.

TABLE I INTERNET APPLICATIONS, PROTOCOLS USED AND PORT NUMBERS

Internet Application	Protocol	Port number
Web browsing	HTTP	80
Name Service	DNS	53
File Transfer	FTP	20,21
E-mail	SMTP POP3	25 110
Secured browsing	HTTPS	443
Boot strapping	BOOTP	67
Net-Bios Name service	NBNS	137

This paper deals with the space and time analysis for internet application identification using port numbers stored using Binary Tree, AVL Tree and Skip List data structures. The applications identified are web browsing, secured web browsing, net-bios and boot strap. The data structures used are analyzed for the space and time efficiency.

### II. BINARY SEARCH TREE, AVL TREE AND SKIP LIST

Data structures can be categorized as static and dynamic. The static data structures include arrays etc, while the dynamic includes Binary search tree, AVL trees etc. There exists different data structures such as linear, trees, hash tables, graphs etc. Linear data structures include arrays, list, etc. Lists contain linked list, skip list, etc. and they are dynamic in nature.

This paper deals with the analysis of space and time for internet application identification using port number by storing the port numbers using skip list, binary search tree and AVL tree.

#### A. Skip list

A skip list stores a sorted list of items. It uses a hierarchy of linked lists which connect increasingly sparse subsequences of the items. The search efficiency or the look up efficiency is  $O(\log n)$ , where  $n$  is number of probes. Each link of the sparser lists skips over many items of the full list



in one step so it is called a skip list. Figure 1 shows the skip list structure [1],[2],[3],[4].

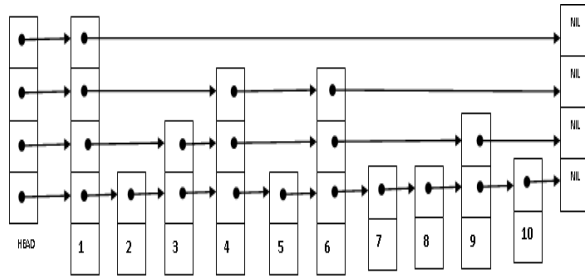


Figure 1. Skip list structure

The forward links are added in a randomized way with a geometric / negative binomial distribution. A skip list is built in layers. The bottom layer is an ordinary ordered linked list. Each higher layer acts as an "express lane" for the lists below, where an element in layer  $i$  appears in layer  $i+1$  with some fixed probability  $p$  (two commonly-used values for  $p$  are  $1/2$  or  $1/4$ ). On average, each element appears in  $1/(1-p)$  lists, and the tallest element (usually a special head element at the front of the skip list) in lists. A search for a target element begins at the head element in the top list, and proceeds horizontally until the current element is greater than or equal to the target. If the current element is equal to the target, it has been found. If the current element is greater than the target, or the search reaches the end of the linked list, the procedure is repeated after returning to the previous element and dropping down vertically to the next lower list.

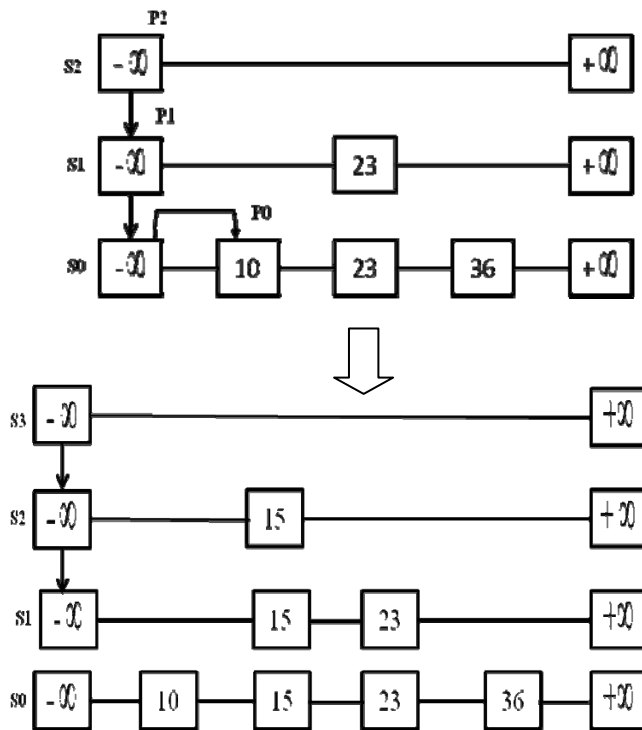


Figure 2. Insertion of element in skip list

The two main operations carried on a skip list are insertion and searching of an element. Suppose a number 15 is to be inserted in the skip list then a spot between 10 and 23 has to be searched and then the number is to be inserted. Figure 2 shows insertion of a number 15 in the skip list.

The expected number of steps in each linked list is at most  $1/p$ , which can be seen by tracing the search path backwards from the target until reaching an element that appears in the next higher list or reaching the beginning of the current list. Therefore, the total expected cost of a search is  $O(\log n)$  when  $p$  is a constant.

To search a key or number say 'x' in the list the search starts at the first position of the top list. At the current position "p", "x" is compared with "y";  
 "x" with "y"  $\leftarrow$  key (after ("p"))  
 "x" = "y" : return element (after("p"))  
 "x" > "y" : scan forward  
 "x" < "y" : drop down

If, after drop down the bottom of the list is reached then no such key exists.

Figure 3 shows search operation for number 78 in skip list. The search will start at S3 number 78 is greater than current position "p",  $-\infty$  so check the next number at same level, its  $+\infty$  which is greater than 78 so drop to the next level S2. Here too the number 78 is compared with  $-\infty$ , then with 31 and then with  $+\infty$ . Then drop to level S1. Here p is 64, at S1,  $+\infty$  is bigger than 78, we drop down at S0, 78 = 78, and the search is completed.

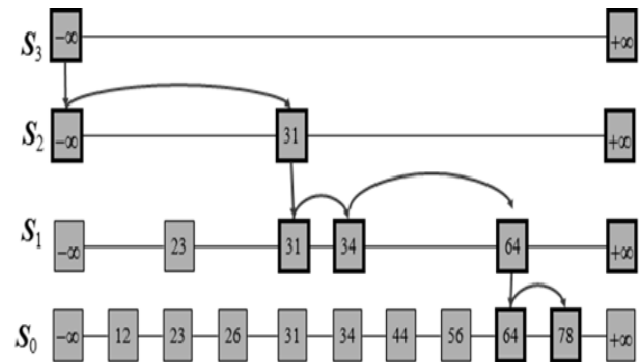


Figure 3. Example of Searching

The number of levels in skip list can vary, as the levels increase the search time reduces. Ideally, a skip list should have  $3(\log n)$  number of levels where  $n$  is the number of elements in the skip list.

#### B. Binary Search Tree (BST)

BST is an ordered or sorted binary tree. It is a node-based binary tree data structure which has the properties like; the left sub tree of a node contains only nodes with keys less than the node's key, the right subtree of a node contains only nodes with keys greater than the node's key. Both the left and right sub trees must also be BST. The information represented by each node is a record rather than a single data

element. BST is a very efficient algorithm. Figure 4 shows a simple BST [3], [5].

### C. AVL Tree

An AVL tree is a self-balancing binary search tree. In an AVL tree, the heights of the two child sub trees of any node differ by at most one. The AVL tree is named after its two Soviet inventors, G. M. Adelson-Velskii and E. M. Landis, who published it in their 1962 paper "An algorithm for the organization of information"[2], [3], [5].

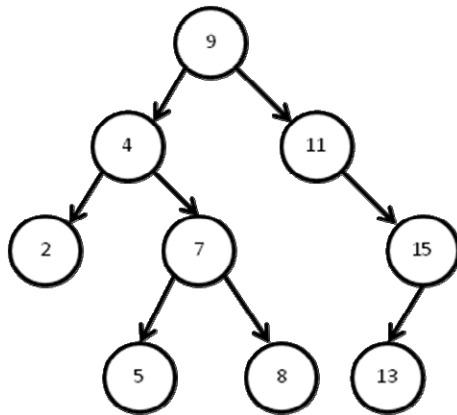


Figure 4. Binary Search Tree

The balance factor of a node is the height of its left subtree minus the height of its right subtree (sometimes opposite) and a node with balance factor 1, 0, or -1 is considered balanced. A node with any other balance factor is considered unbalanced and requires rebalancing the tree. The balance factor is either stored directly at each node or computed from the heights of the sub trees.

AVL trees are often compared with red-black trees because they support the same set of operations and because red-black trees also take  $O(\log n)$  time for the basic operations. Because AVL trees are more rigidly balanced, they are faster than red-black trees.

#### a. Operations performed on AVL

Basic operations of an AVL tree are just the same as unbalanced binary search tree, but modifications are preceded or followed by one or more operations called tree rotations, which help to restore the height balance of the subtrees. The Rotations on AVL and searching operations on AVL are discussed below.

#### b. Rotations on AVL

After inserting a node, it is necessary to check each of the node's ancestors for consistency with the rules of AVL. For each node checked, if the balance factor remains -1, 0, or +1 then no rotations are necessary. However, if balance factor becomes less than -1 or greater than +1, the subtree rooted at this node is unbalanced. If insertions are performed serially,

after each insertion, at most one of the following cases needs to be resolved to restore the entire tree to the rules of AVL.

There are four cases which need to be considered, of which two are symmetric to the other two. Let P be the root of the unbalanced subtree, with R and L denoting the right and left children of P respectively.

#### a) Right-Right case and Right-Left case

If the balance factor of P is -2 then the right subtree outweighs the left subtree of the given node, and the balance factor of the right child (R) must be checked. The left rotation with P as the root is necessary. If the balance factor of R is -1, a single left rotation (with P as the root) is needed (Right-Right case). If the balance factor of R is +1, two different rotations are needed. The first rotation is a right rotation with R as the root. The second is a left rotation with P as the root (Right-Left case).

#### b) Left-Left case and Left-Right case

If the balance factor of P is 2, then the left subtree outweighs the right subtree of the given node, and the balance factor of the left child (L) must be checked right rotation with P as the root is necessary. If the balance factor of L is +1, a single right rotation (with P as the root) is needed (Left-Left case). If the balance factor of L is -1, two different rotations are needed. The first rotation is left rotation with L as the root. The second is a right rotation with P as the root (Left-Right Case).

Figure 5 shows the rebalancing of tree using the rotations and then retracing one's steps toward the root updating the balance factor of the nodes. The numbered circles represent the nodes being balanced. The lettered triangles represent sub trees which are themselves balanced BSTs.

Searching in an AVL tree is performed exactly like in any unbalanced binary search tree. Because of the height-balancing of the tree, it takes  $O(\log n)$  time. No special actions need to be taken, and the tree's structure is not modified by lookups.

If each node additionally records the size of its sub tree, then the nodes can be retrieved by index in  $O(\log n)$  time. Once a node has been found in a balanced tree, the next or previous nodes can be explored in constant time. Some instances of exploring these "nearby" nodes require traversing up to  $2 \times \log(n)$  links particularly when moving from the rightmost leaf of the root's left sub tree to the leftmost leaf of the root's right sub tree. However, exploring all  $n$  nodes of the tree in this manner would use each link exactly twice, one traversal to enter the sub tree rooted at that node, and another to leave that node's sub tree after having explored it.

## III. IMPLEMENTATION AND RESULTS

The data structures AVL tree, Binary Search Trees and Skip list are used to store the data using which the internet application can be identified. Every standardized internet application can be identified using a standard number which

is assigned to the protocol that application uses by the IANA to the protocol used for that application. This number is said to be a port number which is of 16 bits, present at the transport layer of the TCP/IP model and represented in decimal format. The port numbers from 0 to 1023 are well-known port numbers which are assigned to the protocols of standard internet applications. The well known port numbers from are stored using the data structures to form data base for internet application identification. The port number of input query packet is matched with the port numbers stored in database using search algorithms.

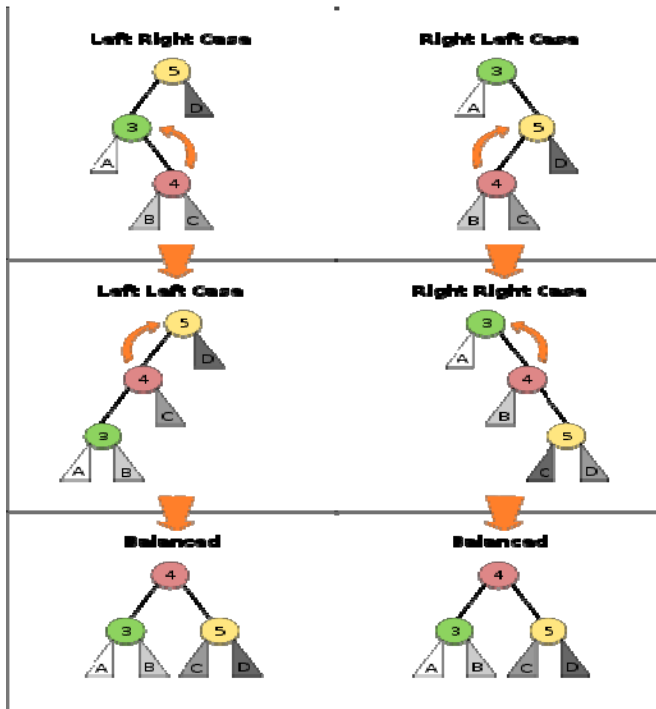


Figure 5. Rotations on AVL

Figure 6 shows mapping of port number extracted from input packet with the database of port number so as to identify application and analyze time required to search the port number and space for data structure and the source code [6], [7],[8].

Data structures and search algorithms are implemented on Linux/Ubuntu platform using 'C' as coding language. The input packets on the network are captured using tcpdump. Skip list is implemented using 5 and 10 levels, BST and AVL are implemented for three traversals in order, preorder and post order, and the results are compared. Analysis of space is done for data structures used for storing the port numbers with the source code and the analysis of time is done for searching port number.

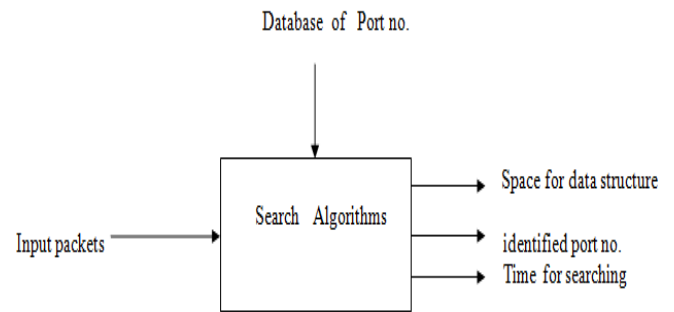


Figure 6. Mapping of input packet with database of port number

The system is tested for active & passive data packets. Applications like web browsing, net-bios, secured browsing and bootstrapping are identified using well-known port numbers 80, 137, 443 and 67 used for the protocols HTTP, NBNS, HTTPS and BOOTP respectively and the packets are stored in separate files named as F1,F2,F3,F4. The unmatched packets are also stored in separate file.

Figure 7 shows a flow diagram implementation of port based internet traffic identification.

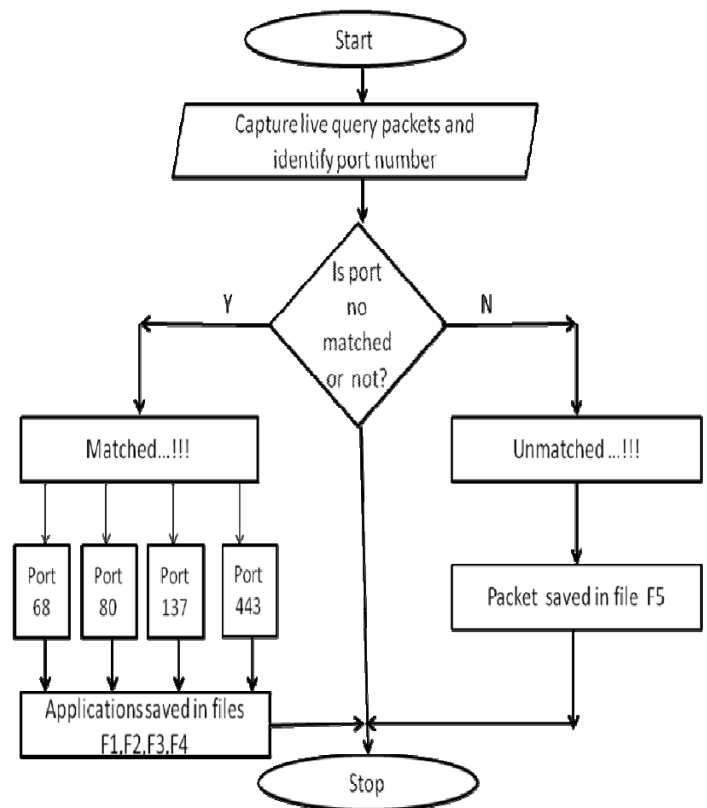


Figure 7. Flow diagram

Table 2 compares the time and space complexity for BST, AVL and Skip list

TABLE II DATA STRUCTURES WITH TIME AND SPACE COMPLEXITY

Data Structures	Time Complexity	Space Complexity
BST	10 Sec	8.1Kb
AVL Tree	06 Sec	10.5Kb
Skip List (with level 5)	11Sec	8.7Kb
Skip List (with level 10)	06 Sec	8.7Kb

### LIMITATION

This identification is implemented only for well-known port numbers. Registered and dynamic port numbers are not considered. The whole analysis is done only for the traffic on college network.

### CONCLUSION

Binary search is faster and doesn't require prior sorting of database. After implementing skip list for different number of levels it is concluded that, as number of levels increases search time reduces. Ideally, number of levels for skip list should be  $3(\log n)$ , where  $n$ = total no of elements in skip list. For  $n=1024$  port numbers, number of levels = 10 requires minimum time for searching an element. Results shows that, searching on AVL tree is more time efficient than BST, as

AVL is height balanced BST. Space requirement for program increases in order as BST, Skip list and AVL tree. Skip list requires optimum space and time.

### REFERENCE

- [1] Amitabha Bagchi, Adam L. Buchsbaum, and Michael T. Goodrich, "Biased Skip Lists", 13th ISAAC, Vancouver, Canada, 2002, Springer-Verlag 2002
- [2] Mark P Neyer, "A Comparison of Dictionary Implementations", April 10, 2009
- [3] Prosenjit Bose, Karim Douieb, Stefan Langerman, "Dynamic Optimality for Skip Lists and B-Trees", nineteenth annual ACM-SIAM symposium on Discrete algorithms Pages 1106-1114 Society for Industrial and Applied Mathematics Philadelphia, PA, USA ©2008
- [4] W. Pugh, "Skip lists: a probabilistic alternative to balanced tree", ACM, volume 33(6), pages 668-676, 1990
- [5] Ben Pfa, "Performance analysis of BSTs in system software", SIGMETRICS '04/Performance '04: Proceedings of the joint international conference on Measurement and modeling of computer systems, pages 410-411, New York, NY, USA, 2004. ACM.
- [6] Pankaj Gupta & Nick McKeown, "Algorithms for Packet Classification", Computer Systems Laboratory, Stanford University Stanford, CA
- [7] V. Shrinivasan, S. Suri, G.Vargese, "Packet classification using tuple space search", Computer Science department, Washington University, St. Louis Research supported in part by NSF grant MCR
- [8] Motasem Aldiab, Emi Garcia-Palacios, Danny Crookes and Sakir Sezer, "Packet Classification by Multilevel Cutting of Classification space: An Algorithm - Architectural Solution for IP packet Classification in Next Generation Networks", Hindawi Publishing Corporation, Journal of Computer Systems, Networks and Communications Vol. 2008, Article ID 603860

# Single MO-CFTA Based Current-Mode SITO Biquad Filter with Electronic Tuning

S. V. Singh

Department of Electronics and  
Communication Engineering, Jaypee  
Institute of Information Technology,  
Sec-128, Noida, India

R. S. Tomar

Department of Electronics  
Engineering, Anand Engineering  
College, Agra, India

D. S. Chauhan

Department of Electrical  
Engineering, Institute of  
Technology, Banaras Hindu  
University, Varanasi-221005 (India),

**Abstract**— This paper presents an electronically tunable current-mode single input three output (SITO) biquad filter employing single multi-output current follower trans-conductance amplifiers (MO-CFTA). The proposed filter employs single resistor and two grounded capacitors. The proposed filter can simultaneously realize low pass (LP), band pass (BP) and high pass (HP) responses in current-mode. It is also capable of providing band reject (BR) and all pass (AP) responses without matching of components. In addition, the circuit possesses low sensitivity performance and low power consumption. The validity of proposed filter is verified through PSPICE simulations.

**Keywords**-component; CFTA, Biquad, Current-mode, Filter

## I. INTRODUCTION

The current-mode filters, where input-output signal is represented by the branch currents of the circuits, have received significant attention owing to their large dynamic range, larger bandwidth, greater linearity, simple circuitry, low power consumption and less chip area over their voltage-mode counterparts, where input-output signal is represented by node voltage of the circuits[1-2]. They can be classified as single-input multiple-output (SIMO) or multiple-input single-output (MISO). There has been a great attention on the design and study of current-mode SIMO filter due to simultaneous realization of multi-function filtering outputs, without changing the connection of the input current signal and without current signal matching. During the last one decade and recent past a number of universal current-mode SIMO active filters have been reported in the literature [3-15, 17-22], using different electronically tunable current-mode active elements such as CCCII [3-6], OTA[7-8], CDTA[9,10,18,21], CFTA[11-13], CCCCTA[14-15], CCTA[17] and VDTA[22] etc. where CCCII, OTA, CDTA, CFTA, CCTA, CCCCTA and VDTA stand for current controlled current conveyor, operational transconductance amplifier, current differencing transconductance amplifier, current follower transconductance amplifier, current conveyor transconductance amplifier, current controlled current conveyor transconductance amplifier and voltage differencing transconductance amplifier, respectively. The current-mode filters reported in Refs.[3-15] realize multi-filtering functions but they contain six [3], five [4], four [12,13], three [5-6,10-11, 14-15], two [9] active elements which are excessive in numbers. On the other hand, the active filter employing low active components is more beneficial from fabrication point of view. Moreover, it can also reduce the power

consumption and the area of chip when it builds in the form of ICs [16]. So several current-mode SIMO filters using single active element (minimum number of active element) have been proposed in the literature [17-22] but most of them [17-20] contain four passive elements (two capacitors and two resistors) while remaining [21-22] consists of three passive elements (two capacitors and one resistors). These circuits [17-22] claim for realizing two [20] or three [17-19] or all five [21-22] filtering functions. However, all the reported filter circuits [17-22] based on single active element provide only one [18, 21, 22] or no [17, 19, 20] filtering function in the form of explicit current output. Explicit current outputs are necessary for the cascading of current-mode filter. In addition, the circuits reported in Refs. [18, 19, 22] do not provide orthogonal electronic tunability of pole frequency and quality factor.

In this paper, a new current-mode biquad filter based on single MO-CFTA is proposed. The proposed filter employs one resistor and two grounded capacitors. The proposed filter can simultaneously realize LP, BP and HP responses in current form in which two of the outputs (LP, BP) are explicitly available. In addition, the pole frequency and quality factor of the proposed current-mode filter circuit can be tuned electronically and orthogonally. The circuit possesses low sensitivity performance and low power consumption. The validity of proposed filter is verified through PSPICE, industry standard tool.

## II. MO-CFTA AND PROPOSED CURRENT MODE FILTER

A MO-CFTA is a combination of current follower and multi-output transconductance amplifier. The properties of ideal MO-CFTA can be characterized by the following set of equations

$$V_f = 0, I_{\pm Z} = \pm I_f, I_{\pm X} = \pm g_m V_Z \quad (1)$$

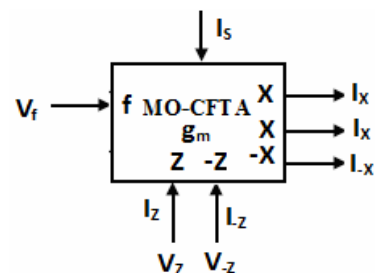


Fig. 1. MO-CFTA Symbol

where  $g_m$  is trans-conductance of the CFTA. The  $g_m$  depends upon the biasing current  $I_S$  of the CFTA. The schematic symbol of CFTA is illustrated in Fig. 1. For MOS implementation of CFTA [10], the  $g_m$  can be expressed as

$$g_m = \sqrt{\beta_n I_S} \quad (2)$$

where  $\beta_n$  is given by

$$\beta_n = \mu_n C_{OX} \left( \frac{W}{L} \right) \quad (3)$$

where  $\mu_n$ ,  $C_{OX}$  are the electron mobility, gate oxide capacitance per unit area and  $W/L$  is the transistor aspect ratio of NMOS, M19 and M20 forming a differential pair in the TA stage of employed MO-CFTA as shown in Fig. 3.

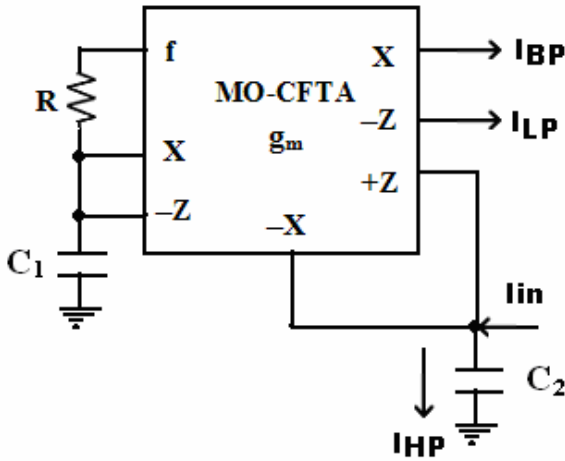


Fig. 2. Proposed MO-CFTA based current-mode biquad filter

The proposed current-mode biquad filter with single input and three outputs is shown in Fig. 2. It is based on single MO-CFTA, single resistor and two grounded capacitors. Routine analysis of the proposed circuit yields the following current transfer functions.

$$\frac{I_{LP}}{I_{in}} = \frac{g_m}{RC_1 C_2 s^2 + Rg_m C_1 s + g_m} \quad (4)$$

$$\frac{I_{BP}}{I_{in}} = \frac{-Rg_m C_1 s}{RC_1 C_2 s^2 + Rg_m C_1 s + g_m} \quad (5)$$

$$\frac{I_{HP}}{I_{in}} = \frac{RC_1 C_2 s^2}{RC_1 C_2 s^2 + Rg_m C_1 s + g_m} \quad (6)$$

It is clear from (4) – (6) that the proposed current-mode filter can realize LP, BP and HP responses. The circuit is also capable of realizing BR and AP by adding  $I_{LP}$ ,  $I_{HP}$  and  $I_{LP}$ ,  $I_{HP}$ ,

$I_{BP}$  together, respectively. The pole frequency ( $\omega_0$ ) and quality factor ( $Q$ ) of the proposed circuit is given by

$$\omega_0 = \sqrt{\frac{g_m}{RC_1 C_2}} = \sqrt{\frac{(\beta_n I_S)^{\frac{1}{2}}}{RC_1 C_2}} \quad (7)$$

$$Q = \sqrt{\frac{C_2}{Rg_m C_1}} = \sqrt{\frac{(\beta_n I_S)^{\frac{1}{2}}}{R} \frac{C_2}{C_1}} \quad (8)$$

From (7) and (8), it can be remarked that both the  $\omega_0$  and  $Q$  can be electronically tuned through biasing current  $I_S$ . In addition,  $\omega_0$  and  $Q$  are orthogonally adjustable with adjustment of  $g_m$  and  $R$  such that product  $g_m R$  remain constant and quotient  $g_m/R$  varies and vice versa. The active and passive sensitivities of the proposed circuit as shown in Fig. 2, can be found as

$$S_{C_1, C_2, R}^{\omega_0} = -\frac{1}{2}, S_{\beta_n, I_S}^{\omega_0} = \frac{1}{4} \quad (9)$$

$$S_{C_1, R}^Q = -\frac{1}{2}, S_{\beta_n, I_S}^Q = -\frac{1}{4}, S_{C_2}^Q = \frac{1}{2} \quad (10)$$

From the above results, it can be observed that all the active and passive sensitivities are low and within half in magnitude.

### III. SIMULATION RESULTS

In order to confirm the practical validity of the proposed filter circuit, it was simulated in PSPICE using the MOS implementation of MO-CFTA as shown in Fig. 3, with the transistor model of 0.35 $\mu$ m MOSFET from TSMC whose model parameters are given in Table 1. DC power supplies were selected as  $V_{dd} = -V_{ss} = 1.5V$  and  $V_{bb} = 0.45V$ . To obtain  $f_0 = \omega_0/2\pi = 1.35MHz$  at  $Q=1$ , the active and passive components were chosen as  $I_S = 50.5\mu A$ ,  $R = 6K$  and  $C_1 = C_2 = 20pF$ . Aspect ratio of MOS transistor is given in Table 2. Fig. 4 shows the simulated current gain responses of the LP, BP and HP of the proposed filter. Fig. 5 shows the gain and phase responses of BR and AP filtering functions. The simulation results show the simulated pole frequency as 1.29 MHz that is ~4% in error with the theoretical value. The power dissipation of the proposed circuit for the design values was found as 1.18 mW that is a low value. Next, the tuning aspect of pole frequency was tested for constant  $Q (=1)$  through simulation of BP responses. The bias current  $I_S$  ( $g_m$ ) and  $R$  were varied for three sets of values in such a way so that  $g_m R$  remain constant and other parameters were chosen as  $C_1 = C_2 = 20pF$ . The pole frequency variation is shown in Fig. 6. The pole frequency was found to vary as 620 KHz, 1.29 MHz and 1.96 MHz for three different sets of values of  $I_S$  ( $g_m$ ) and  $R$  as mentioned in Fig. 6. Similarly, Fig. 7 shows the gain responses of BP function, for different values of  $R$  and  $I_S$  to indicate the tuning of quality factor of the proposed filter circuit, with out affecting the pole frequency.

Identify applicable sponsor/s here. (sponsors)

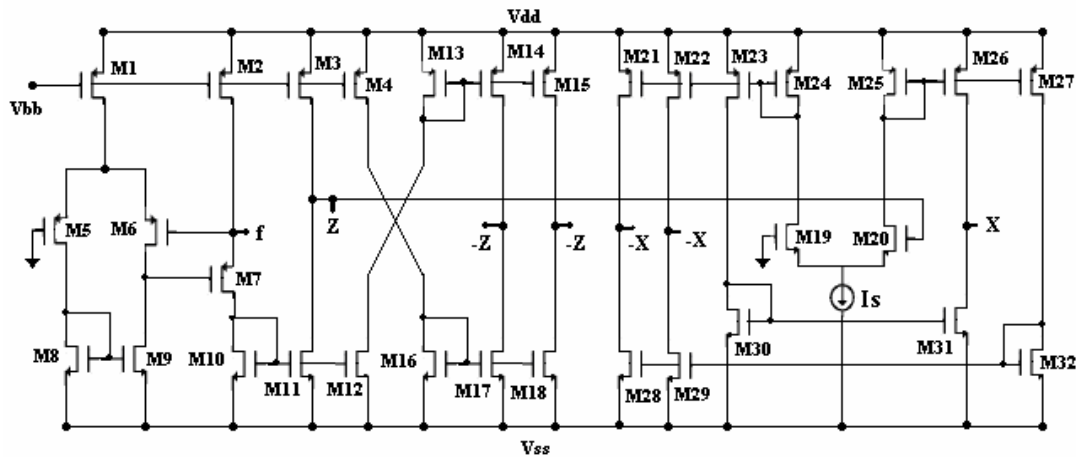


Fig. 3. CMOS Implementation of MO-CFTA

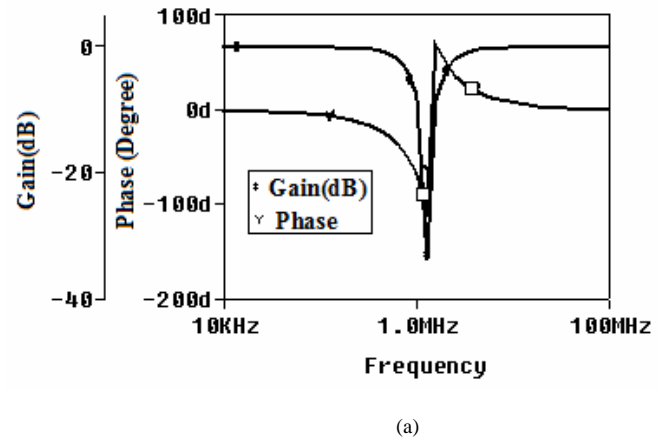
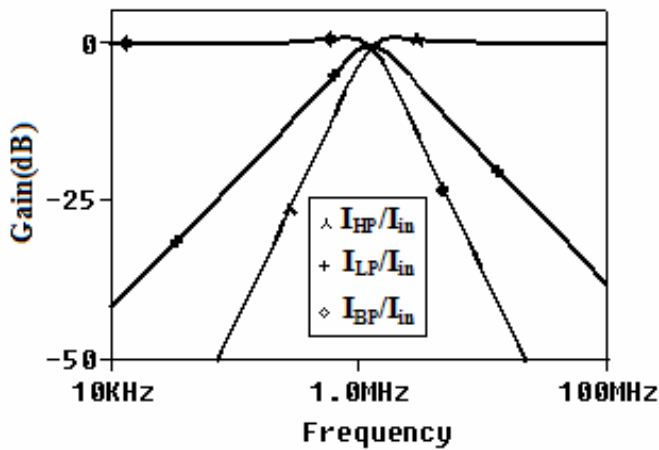


Fig. 4. Gain responses of LP, BP and HP for the proposed current-mode filter

Further, simulations were carried out to verify the total harmonic distortion (THD). The circuit was verified by applying a sinusoidal voltage ( $I_{in}$ ) of varying frequency and amplitude of  $20\mu A$ . The THD measured at the LP output were found to be less than 4% while frequency was varied from 100 KHz to 500 KHz. The time domain behavior of the proposed current-mode filter was also investigated by applying a 500 KHz sinusoidal input current signal with peak to peak amplitude of  $40\mu A$ . Fig. 8 shows the time domain sinusoidal current input and corresponding LP output waveform for the proposed filter.

Further, the Monte Carlo analysis of the proposed circuit for  $C_1 = C_2 = 20$  pF was also performed taking 15% tolerances in the capacitive components. The analysis was done for six runs. The time domain response of current-mode LP output ( $I_{LP}$ ) is shown in Fig. 9. It is observed that  $40\mu A$  peak to peak input current sinusoidal signal levels having frequency 500 KHz are possible without significant distortions.

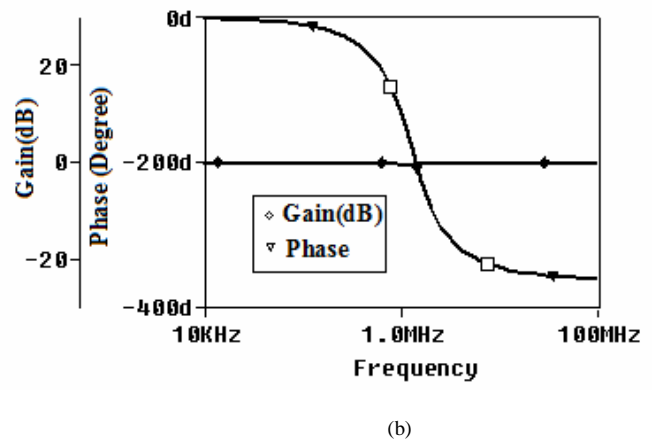


Fig. 5. Gain and phase response of (a) BR and (b) AP filtering functions for the proposed current-mode filter



Table 1. The SPICE model parameters of MOSFET for level 3, 0.35  $\mu\text{m}$  CMOS process from TSMC

NMOS	LEVEL=3 TOX=7.9E-9 NSUB=1E17 GAMMA=0.5827871 PHI=0.7 VTO=0.5445549 DELTA=0 UO=436.256147 ETA=0 THETA=0.1749684 KP=2.055786E-4 VMAX=8.309444E4 KAPPA=0.2574081 RSH=0.0559398 NFS=1E12 TPG=1 XJ=3E-7 LD=3.162278E-11 WD=7.046724E-8 CGDO=2.82E-10 CGSO=2.82E-10 CGBO=1E-10 CJ=1E-3 PB=0.9758533 MJ=0.3448504 CJSW=3.777852E-10 MJSW=0.3508721
PMOS	LEVEL=3 TOX=7.9E-9 NSUB=1E17 GAMMA=0.4083894 PHI=0.7 VTO=-0.7140674 DELTA=0 UO=212.2319801 ETA=9.999762E-4 THETA=0.2020774 KP=6.733755E-5 VMAX=1.181551E5 KAPPA=1.5 RSH=30.0712458 NFS=1E12 TPG=-1 XJ=2E-7 LD=5.000001E-13 WD=1.249872E-7 CGDO=3.09E-10 CGSO=3.09E-10 CGBO=1E-10 CJ=1.419508E-3 PB=0.8152753 MJ=0.5 CJSW=4.813504E-10 MJSW=0.5

Table 2. Dimensions of MOS Transistors

NMOS Transistors	W ( $\mu\text{m}$ ) / L ( $\mu\text{m}$ )
M8-M12 & M16-M18	0.7 / 0.35
M19, M20	4.0 / 1.0
M28-M32	4.0 / 1.0
PMOS Transistors	W ( $\mu\text{m}$ ) / L ( $\mu\text{m}$ )
M1,M5,M6	1.4 / 0.35
M7	5.6 / 0.35
M2-M4 & M13-M15	2.8 / 0.35
M21-M27	4.0 / 1.0

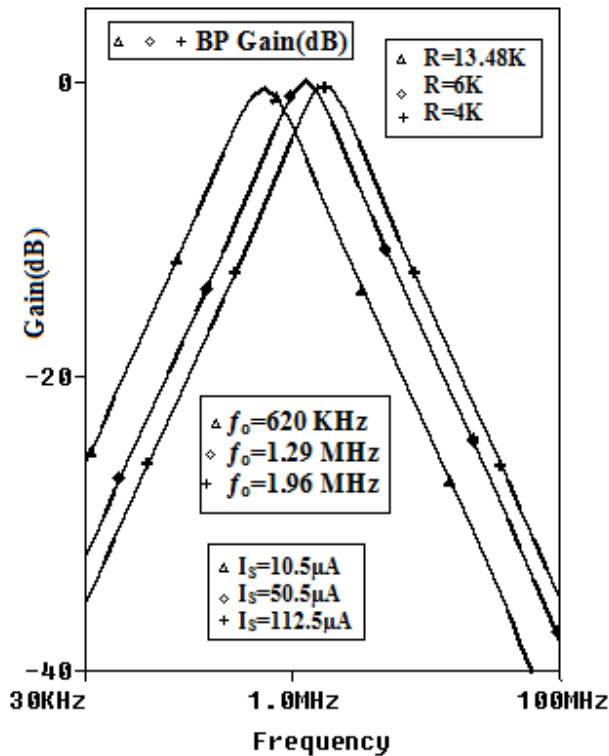


Fig. 6. BP responses showing pole frequency tuning

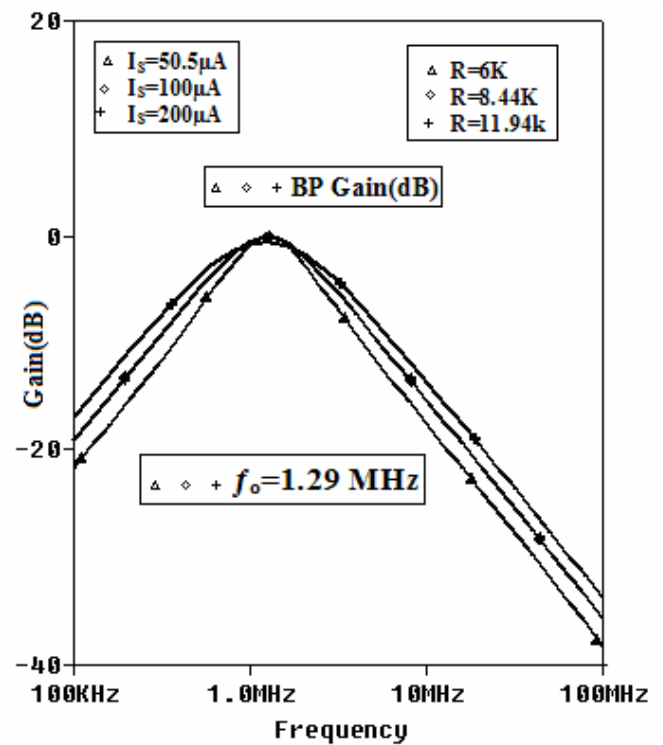


Fig. 7. BP responses showing quality factor tuning

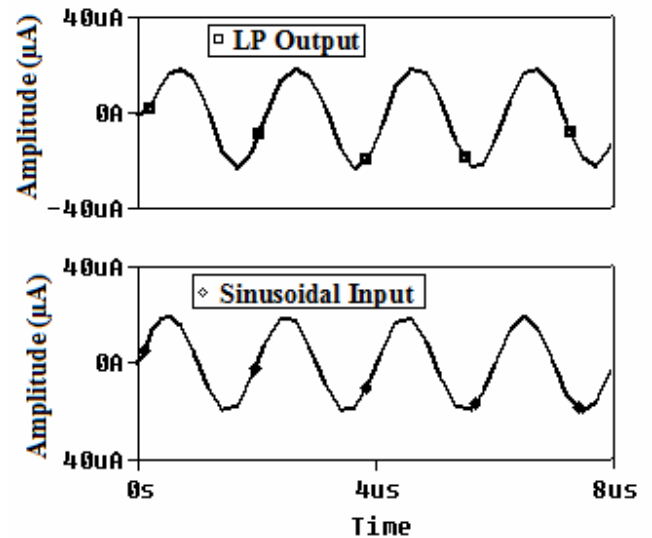


Fig. 8. The time domain sinusoidal current input and corresponding current-mode LP output

#### IV. CONCLUSION

In this paper, an electronic tunable current-mode biquad filter with single input and three outputs using only single MO-CFTA, one resistor and two grounded capacitors has been presented. The proposed current-mode filter can simultaneously realize LP, BP and HP responses. it is also capable of realizing BR and AP



filtering functions. In additions, it also offers several advantages, such as orthogonal electronic tunability of  $\omega_0$  and  $Q$ , the use of grounded capacitors, low active and passive sensitivities.

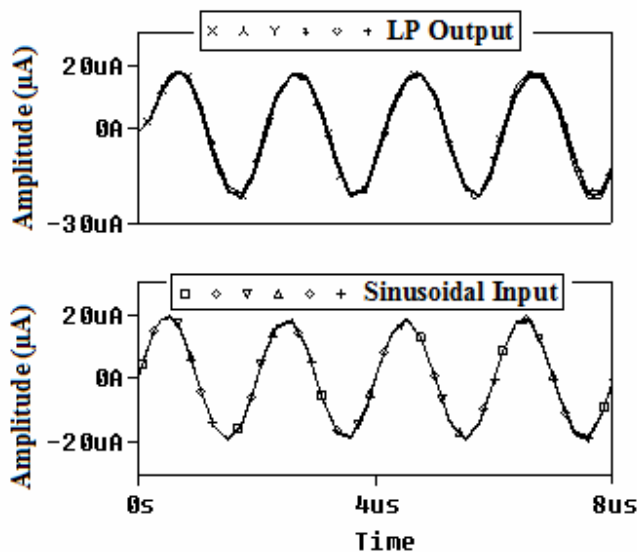


Fig. 9. The time domain sinusoidal current input and corresponding current-mode LP output for Monte Carlo analysis

#### REFERENCES

- [1] B. Wilson, "Recent developments in current mode circuits," Proc. IEE., Pt. G, vol. 137, pp. 63-77, 1990.
- [2] G. W. Roberts and A. S. Sedra, "All current-mode frequency selective circuits," Electronics Lett., vol. 25, pp. 759-761, 1989.
- [3] M. T. Abuelma'atti and N. A. Tassaduq, "A novel single-input multiple-output current-controlled universal filter," Microelectronics J., vol. 29, pp. 901-905, 1998.
- [4] S. Minaei and S. Türköz, "New current-mode current-controlled universal filter with single input and three outputs," Int'l J. Electronics, vol. 88, pp. 333-337, 2001.
- [5] S. Maheshwari and I. A. Khan, "Novel cascaded current-mode translinear-C universal filter," Active Passive Electronic component, vol. 27, pp. 215-218, 2004.
- [6] R. Senani, V. K. Singh, A. K. Singh, and D. R. Bhaskar, "Novel electronically controllable current mode universal biquad filter," IEICE Electronics Express, vol. 1, pp. 410-415, 2004.
- [7] T. Tsukutani, M. Ishida, S. Tsuiki and Y. Fukui, "Versatile current-mode biquad filter using multiple current output OTAs," Int'l J. Electronics, vol. 80, no. 4, pp. 533-541, 1996.
- [8] D. R. Bhaskar, A. K. Singh, R. K. Sharma and R. Senani, "New OTA-C universal current-mode/trans-admittance biquads," IEICE Electronic Express, vol. 2, no. 1, pp. 8-13, 2005.
- [9] A. U. Keskin, D. Biölek, E. Hancioglu and V. Biolkova, Current-mode KHN filter employing current differencing transconductance amplifiers, Int'l J. Electronics and Communications (AEÜ), vol. 60, pp. 443-446, 2006.
- [10] D. Biölek and V. Biolkova, "CDTA-C current-mode universal 2<sup>nd</sup> order filter," Proceeding of the 5<sup>th</sup> Int. Conf. on Applied Informatics and Communications, pp. 411-414, 2003.
- [11] N. Herencsar, J. Koton, K. Vrva and A. Lahiri, "Novel mixed-mode KHN equivalent filter using Z-copy CFTAs and Grounded Capacitors," Latest Trends On Circuits, Systems and Signals, pp. 87-90, 2010.
- [12] J. Satansup and W. Tangsrirat, "Single input five output electronically tunable current-mode biquad consisting of only ZC-CFTAs and grounded capacitors," Radioengineering J., vol. 20, pp. 273-280, 2011.
- [13] W. Tangsrirat, "Single input three output electronically tunable universal current-mode filter using current follower transconductance amplifiers," Int'l J. Electronics and communication (AEU), doi: 10.1016/j.aeu.2011.01.002.
- [14] S. Maheshwari, S. V. Singh and D. S. Chauhan, "Electronically tunable low voltage mixed-mode universal biquad filter," IET Circuits, Devices and Systems, vol. 5, no. 3, pp. 149-158, 2011.
- [15] S. V. Singh, S. Maheshwari and D. S. Chauhan, "Universal current-controlled current-mode biquad filter employing MO-CCCCTAs and grounded capacitors," J. Circuits and Systems, vol. 1, pp. 35-40, 2010.
- [16] M. Kumngern, U. Torteanchai and K. Sarsithithum, "Current-tunable current-mode multifunction filter employing a modified CCCCTA," 7<sup>th</sup> IEEE Int. Conf. On Industrial Electronics and Applications (ICIEA), pp. 1794-1797, 2011.
- [17] N. Herencsar, J. Koton and K. Vrva, "Single CCTA-based universal biquad filters employing minimum components," Int'l J. Computer and Electrical Engineering, vol. 1, pp. 307-310, 2009.
- [18] D. Prasad, D. R. Bhaskar and A. K. Singh, "Universal current-mode biquad filter using dual output current differencing transconductance amplifier," Int'l J. Electronics and communication (AEU), vol. 63, pp. 497-501, 2009.
- [19] B. Chaturvedi and S. Maheshwari, "Current-mode Biquad filter with minimum component count," Active and Passive Electronic Components, vol. 2011, pp. 1-7, doi:10.1155/2011/391642.
- [20] E. Yuçe, B. Metin and O. Cicekoglul, "Current-mode Biquadretic filters using single CCII and minimum number of passive elements," Frequenz: Journal Of RF-Engineering and Telecommunication, vol. 58, pp. 225-227, 2004.
- [21] N. A. Shah, M. Quadri, S. Z. Iqbal, "Realization of CDTA-based current-mode universal filter," Indian J. Pure and Applied Physics, vol. 46, pp. 283-285, 2008.
- [22] D. Prasad, D. R. Bhaskar and M. Srivastava, "Universal current-mode biquad filter using a VDTA," J. Circuits and Systems, vol. 4, pp. 32-36, 2013.

#### AUTHORS PROFILE

**S. V. Singh** was born in Agra, India. He received his B.E. degree (1998) in Electronics and Telecommunication from NIT Silchar, Assam (India), M.E. degree (2002) from MNIT Jaipur, Rajasthan (India) and Ph.D. degree (2011) from Uttarakhand Technical University. He is currently working as Assistant Professor in the Department of Electronics and Communication Engineering of Jaypee Institute of Information Technology, Noida (India) and has been engaged in teaching and design of courses related to the design and synthesis of Analog and Digital Electronic Circuits. His research areas include Analog IC Circuits and Filter design. He has published more than 20 research papers in various International Journal/Conferences.

**R. S. Tomar** was born in Aligarh, India. He obtained his B. E (1995) from Bombay University, M. E. (2004) from Agra. He is currently associated with Anand Engineering College, Agra. His research areas include designing of microwave and analog circuits. He has published no. of papers in National and International Conferences.

**D. S. Chauhan** was born in Dholpur, India. He obtained his B.Sc Engg.(1972) in Electrical Engineering at I.T. B.H.U., M.E. (1978) at R.E.C. Tiruchirapalli ( Madras University ) and Ph.D. (1986) at IIT/Delhi. His brilliant career brought him to teaching profession at Banaras Hindu University where he was Lecturer, Reader and then has been Professor till today. He has been director KNIT Sultanpur in 1999-2000 and founder vice Chancellor of U.P.Tech. University (2000-2003-2006). Later on, he has served as Vice-Chancellor of Lovely Professional University (2006-07) and Jaypee University of Information Technology (2007-2009). Currently he has been serving as Vice-Chancellor of Uttarakhand Technical University. He has supervised 24 Ph.D., one D.Sc. He has authored two books and published and presented 170 research papers in international journals and international conferences. His research areas include Analog IC Circuits and Control Systems design.

# Dynamic AODV for Mobile Ad-hoc Network

Aditya Shrivastava  
Information Technology  
TIT, Bhopal, India

Deepshikha Patel  
Information Technology  
TIT, Bhopal, India

Amit Sinhal  
Information Technology  
TIT, Bhopal, India

**Abstract:** Since long time work has been done to enhance working capability of AODV (Ad-hoc on demand distance vector routing protocol for Mobile Ad-hoc Network). Performance of AODV has been improved by some modification in its working procedure by many others researchers. Few parameters have been improved, and rest has been trade-offs. In this research work, AODV has been modified in such a way to improve its Dynamistic. Obviously, performance has been improved in terms of Throughput and Packet Delivery Ratio with the compromising Avg, End to End Delay and Routing/Network Overhead.

**Keywords:-** AODV, PDR, Networks Overhead, Throughputs, Avg. End-To-End Delay, Dynamic.

## I. INTRODUCTION

It is very common in any environment to set up a temporary network for a particular task, and also it takes small time to perform the work assigned using Mobile Ad-hoc Network. The Ad-hoc network is an Infrastructure fewer networks, in which nodes communicate with each other through a wireless medium without any centralized monitoring body [1]. The nodes in ad-hoc networks can be stationary or mobile, the latter being the most common situation. The absence of the centralized infrastructure implies that the responsibility of the nodes is equal [2]. Therefore, participating nodes on the network need to cooperate in order to establish routes and to forward packets to other nodes [3]. The nodes use routing protocols to establish and maintain the routes. The commonly used standard for ad-hoc networks is IEEE802.11b [4].

Suppose we have three nodes A,B & C. The node B relays messages between A and C. Supposed A is source and C is destination and B is the node between A and C. In networks that are, more complex packets from the source node can traverse several multi-hop routes in order to reach the destination node.

Research has been contributed in [7] Mobile ad hoc network has grouped of the wireless nodes. They are communication without a centralized mechanism for the network. There are various issues in the mobile ad-hoc network in one of them is energy. The outcome of the algorithm does have a positive result in ns2. The further research issue is to develop an optimal model through applying various parameters in different environments. This Research has been contributed in [8]. In on demand distance vector routing in MANET establish is a single

path for the communication. This paper introduces novel on-demand due to multipath routing protocol for MANET, which combines the metrics of delay, hop count and disjointness; each intermediate node deliberately selects multipath candidates while.

contributing to suppression of unnecessary routing packets. To the extension of the RREQ / RREP packet provide more efficient multipath routes. The outcome of this research has a higher packet delivery ratio and lower routing packets. This Research has been contributed in. Ad-hoc networks are characterized by multi-hop wireless connectivity and frequently changing network topology, which have made infrastructure less. In this research compares of the AODV, DSR and TORA routing protocols with respect to a modified path optimality that we call as weighted path optimality and analyse various factors average end-end delay and jitter, etc. This Research has been contributed in An Ad-hoc network is the collection of mobile nodes communicating without a centralized infrastructure. MANET generally uses a wireless radio communication channel. So they are open to various types of attack. The outcome of this research performance of AODV is improved. Future direction of the research is looking for the solution of some kinds of attack (i.e. wormhole, Flooding, Black hole etc.) on Routing protocols in Ad-hoc Network In MANET routers have recreated many times due to the mobility of the nodes. If a node in a mobile ad hoc network aware of the mobility of the neighbor nodes then highly mobile node is to avoid becoming a part of routes, this will greatly reduce new path discovery towards the destination.

## II. LITRATURE SURVEY

Sung-Ju Lee et-all in [5] presented an algorithm which establishes the mesh and multipath without transmitting any extra control message.

Neda Moghim et-all in [7] has tried to reduce AODV's routing load by preventing AODV from relying on route request flood more often in the route discovery process.

Q. Wang et-all in [8] presents a new scheme AO-DVRR (Ad Hoc On-demand Distance Vector Protocol with Redundant Routes) with improved robustness, but the overhead is increases.

Zhao Qiang Zhu Hongbo et-all in [12] proposes a new scheme to improve AODV protocol by the concept of reliable distance, and the path selected but the complexity of the algorithm increases.

Dr. S. A. Hussain et-all in [11] shows that if a node in a mobile ad-hoc network aware of the mobility of the neighbor nodes, then highly mobile node should be avoided

to become a part of shortest routes. This will greatly reduce new path discovery towards the destination, but extra hello packets are required to achieve this mechanism.

Vahid Nazari Talooki et-al in [10] compare the AODV, DSR and TORA routing protocols with respect to a modified path optimality based on average end-to-end delay and other parameters by which they analyze protocols performance.

Azzedine Boukerche et-al in [6] presented extensive simulation studies to compare three ad-hoc protocols, DSR, AODV, and CBRP using a variety of work load such mobility, load and size of the ad-hoc networks

Jagpreet et-al in [1] shows an enhance local repair AODV is based on the local repair strategy where unicast mechanism has been introduced to improve the routing overhead by making mobile nodes aware of local connectivity. In the proposed Methodology, it extended the HELLO packet to NHellow this extra information helps AODV to repair the route by unicast instead of broadcast but end-to-end delay and routing overhead increases.

Umang Singh et.al in [16] Shows a good node detection strategy on the basis of value of packet delivery ratio and network range, but it does not comments on type of bad node.

### III. PROPOSED WORK AND ALGORITHM.

In AODV, we know that we use flooding of RREQ towards the destination for the shortest route discovery in on demand routing protocol as in AODV. Destination reply by RREP which contained shortest route then sources send Data packet and wait for Acknowledgment.

In this work, we have proposed a solution for next shortest path recovery, which is only possible when a node kept an address of more than one nearest node. Which can be used as a mediator node in case of failure of a shortest path intermediate node? Modified AODV should have adopted the capability of choosing the next nearest node which comprises of a next shortest path.

#### A. PROPOSED WORK:

In AODV, we know that we use flooding of RREQ towards the destination for the shortest route discovery in on demand routing protocol as in AODV. Destination reply by RREP which contained shortest route then sources send Data packet and wait for Acknowledgment.

In this work, we have proposed a solution for next shortest path recovery, which is only possible when a node kept an address of more than one nearest node. Which can be used as a mediator node in case of failure of a shortest path intermediate node? Modified AODV should have adopted the capability of choosing the next nearest node which comprises of a next shortest path.

#### B. PROPOSED ALGORITHM:

**Step 1:** Initialize Credit Value of each node (Say N)

**Step 2:** Broadcasted RREQ message to discover a route and decrease the Credit Value (CV) of each node by -1 ( $CV = N-1$ )

**Step 3:** If RREQ message is received by destination, then shortest path is made available by uni-casting a RREP back to the source route (It makes two entries in the routing table one is for next node, and another is for the node there after) and increase Credit Value of each node in the shortest path by +2 and Go to step 8.

**Step 4:** Source node will send Data Packet to the Destination node using the shortest path.

**Step 5:** If a link is broken, then apply the local route repair mechanism to recover the route.

**Step 6:** If a route is available after local route repair, then sends a data packets through repaired path and Go to step 8. Else forward data packet to next to next node for successful transmission.

**Step 7:** If a route is available, then send a data packets through the repaired path.

**Step 8:** Observed the credit value at each node in the shortest path.

**Step 9:** If the credit value is  $\leq (N-10)$ , then declare the node as a bad nodes.

**Step 12:** If the credit value is  $\geq (N+10)$  then declare the node as good node and go to step 14.

**Step 13:** Send PSRERR to source node, If the first bit of the PSRERR packet is 1, then it prioritize a packet, if the second bit is also 1, then it is having information about bad node or attackers.

**Step 14:** end

#### c. Performance Analysis:

Results of simulation have been analyzed as the basis of following parameters using Standard Network Simulator (Freely Available) N.S-2.34 [9].

- **End-to-end delay:** It refers to the time taken for a packet to be transmitted across a network from source to destination.
- **Routing Overhead:** It refers to metadata and network routing information sent by an application, which uses a portion of the available bandwidth of a communications protocol. This extra data, making up the protocol headers and application-specific information are referred to as overhead, since it does not contribute to the content to the message.
- **Throughput:** No. of packet transmitted per unit of time.

$$\text{Throughput} = \text{Data Packet Transmitted} / \text{Time} \dots (1)$$

- **Packet Delivery Ratio:** It is defined as the ratio of packet received to packet transmitted. Generally represent in percentages. If Packet Transmitted=Pts, and Packet received is Pr, Then.

$$\text{PDR (\%)} = \text{Pr/Pt} * 100 \dots \dots \dots (2)$$

**D. Performance Matrix:**

<b>Transmitter Range</b>	<b>300 m</b>
<b>Bandwidth</b>	<b>2Mbits/s</b>
<b>Simulation Time</b>	<b>90 msec</b>
<b>Number of nodes</b>	<b>10 to 50</b>
<b>Scenario size</b>	<b>500 x 500 m2</b>
<b>Traffic type</b>	<b>CBR</b>
<b>Packet size</b>	<b>64 bytes</b>
<b>Rate</b>	<b>25 packets/s</b>

Table 1: Simulation Parameters

**IV. RESULTS ANALYSIS:**

Based on simulation using NS-2.34 results has been evaluated and compared with AODV using four well known Key Performances Indicators, i.e. Throughput, Packet Delivery Ratio, End-to-End Delay, Overhead.

- **Throughputs:** Table 2 shows improvement in MAODV (Modified AODV) in terms of Throughputs.

S.No	No of Nodes	Throughput	
		AODV	Orn-AODV
1	5	109.3	115.6
2	10	104.84	116.5
3	15	90.18	118.4
4	25	123.5	135.7
5	40	126.2	133.6

Table 2: Throughput Comparison

**Throughput Improvement has been found due to choosing addresses of another nearest node for completion of the shortest path if one node has been a failure.**

- **PDR (Packet Delivery Ratio):** Table 2 that PDR is increases whenever we use MAODV. The Received packets increases because of early information about path failure using prioritized control packet and also by utilizing the same optimal path using next to next node.

S.No	No of Nodes	PDR (%)	
		AODV	Orn-AODV
1	5	0.30	0.41
2	10	0.45	0.52
3	15	0.35	0.45
4	25	0.40	0.51
5	40	0.25	0.30
6	50	0.37	0.39

Table 3: Packet Delivery Ratio

Performance of Modified AODV is better in case of low nodes. Whenever nodes during RREP control packet transmissions. Increased performance degraded because of obvious congestion in the networks, but still it is better than AODV. PDR is always best in case of MAODV because of more packet transmissions through the almost same path as suggested by Destination node.

In both case performance of MAODV is always better than AODV, which shows importance and contribution in this research work.

- **Network Overhead:** It can be seen Table 3 that network overhead is almost unchanged because no extra control packet has been transmitted for the information about bad and good node. Previously used REER packet have been modified to inform about priority of control packet.

S.No	No of Nodes	Network Overhead	
		AODV	MAODV
1	5	4.00	4.00
2	10	09.0	10.0
3	15	16.0	17.0
4	25	25.0	26.0
5	40	50.0	51.0
6	50	70.0	72.0

- **Avg. End-to-End Delay:** It can be seen in the Table 4 that Average End-to-End Delay is increases whenever we use Orn-AODV, because of extra calculations performed by each node to know about behavior of nodes In every research work, there is some benefit and some loses this is a drawback of this research work.

S.No	No of Nodes	End-to-End Delay (in ms)	
		AODV	Orn-AODV
1	5	0.01	0.02
2	10	0.05	0.40
3	15	0.12	0.43
4	25	0.06	0.50
5	40	0.02	0.60
6	50	0.52	0.80

Table 4: Avg. End-To-End Delays

Delay is increases because of extra control packets transmitted within the same channel but Throughput and PDR increase, so there is a tradeoff between these parameters this delay is small in case of MAODV and AODV but whenever we increase the number of nodes, these delay increases and difference between both the protocol become wider than at its low values.

## V. CONCLUSION & FUTURE WORK

### A. FUTURE WORK

Basic working procedure of AODV has been modified in such a way to improve its performance in Mobile ad-hoc Networks. It has been observed that throughput increases in the case of proposed Orn-AODV (Modified AODV). Improvement in Throughput has been found due to choosing a next closest node for completion of the path if one node has been a failure. We have given an alternate option to complete the path to use the almost same shortest path is using the address of next closest node, and also simultaneously this

node will inform to all other nodes by flooding the control packet with higher priority than data packets to other nodes.

Also PDR (Packet Delivery Ratio) is increases whenever we use Orn-AODV. Performance of Modified AODV is better in case of low nodes. When nodes increase performance degraded because of obvious congestion in the networks, but sill it is better than AODV. .

### B. FUTURE WORK

Following suggestions have been made here with future work to enhancing the performance of AODV, Routing protocol for ad-hoc networks: In Future Proposed solution may be tested in a real environment. Therefore, future studies should rather be devoted to real implementation than a simulation. Only such an approach can ultimately verify a protocol's utility in future Ad-hoc network. Along with it should be kept in mind that the trade-off between signal strength, routing overhead, congestion, energy, security and Quality of services are challenging issues to resolve all problems together. However, the list is still open for continuous emerging new technology in Ad-hoc Network.

Performance of Arn-AODV has to be evaluated in future in the presence of different types of attackers.

### REFERENCES

- [1] J. Singh, P. Singh and S. Rani, "Enhanced Local Repair AODV (ELRAODV)" IEEE International Conference on Advances in Computing, Control, and Telecommunication Technologies, 12 January 2010 , pp. 787-2010.
- [2] W. Ningning and C. Yewen, "Improved AODV protocol with Lower Route Cost and Smaller Delay" , IEEE Fourth International Conference on Intelligent Computation Technology and Automation ,15 April 2011, pp. 7-11.
- [3] H. Rehman and L. Wolf, "Performance Enhancement in AODV with Accessibility Prediction" , IEEE International Conference on Sensor Network , 12 January 2008, pp. 1-6.
- [4] S. Mittal and P. Kaur, "Performance Comparison Of AODV, DSR and ZRP Routing Protocols In MANET'S" , IEEE International Conference on Advances in Computing Control and Telecommunication ,12 January 2010, pp. 165-169.
- [5] S.J. Lee and M. Gerla, "AODV-BR: Backup Routing in Ad hoc Networks", IEEE Wireless Communication and Networking Conference, Vol. 3 January 2000 , pp. 1311-1316.
- [6] A. Boukerche, "A Simulation Based Study of On-Demand Routing Protocols for Ad-hoc Wireless Networks" , IEEE Simulation Symposium, January 2008 , pp. 85-93.

[7] N. Moghim, "An Improvement On Ad-hoc Wireless Network Routing Based On AODV", The 8<sup>th</sup> International Conference Communication Systems, ICCS 2010, vol.2 , November 2010, pp. 1068 – 1070.

[8] Q. Wang, "A Robust Routing Protocol For Wireless Mobile Ad-hoc Networks", The 8th International Conference on Communication Systems, vol.2 , 25 Nov 2010, pp. 1071–1075.

[9] Yusuke, "AODV Multipath Extension uses Source Route Lists with Optimized Route Establishment", International Workshop on Wireless Ad-hoc Networks, 3 June 2004, pp. 63 – 67.

[10] V.N. Talooki, "Performance Comparison of Routing Protocols For Mobile Ad-hoc Networks", Asia-Pacific Conference on Communications (APCC' 10), 1 September 2010, pp. 1 – 5.

[11] S.A. Hussain, E. Garcia and M. Idrees, "Throughput Enhancement in AODV Routing Using Mobility Awareness", 9th International Multi Topic Conference, IEEE INMIC 2005, July 2005, pp. 1-4.

[12] Z. Qiang and Z. Hongbo, "An optimized AODV protocol in mobile ad hoc Network", IEEE , April 2004 , pp. 1-4.

[13] A. Klein, "Performance Comparison and Evaluation of AODV, OLSR, and SBR in Mobile Ad-Hoc Networks", IEEE , Wireless Pervasive Computing 2008 (ISWPC 2008), Jan 2008 , pp. 571-575.

[14] H.P. Wang and L. Cui, "An Enhanced AODV for Mobile Ad-hoc Network", Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, Kunming, 15 July 2008.

[15] K. Agarwal and L.K. Awasthi, "Enhanced AODV Routing Protocol for Ad hoc Networks" , 16<sup>th</sup> International Conference on Networks (ICON 2008) , 12 December 2008, pp. 1-5.

[16] Umang Singh, B. V. R. Reddy, M. N. Hoda, "GNDA: Detecting good neighbour nodes in ad-hoc routing protocol," Second International conference of Emerging Trend in Information Technology, pp. 235-238, 2011.

# Steganography in Colored Images

Iman Thannoon Sedeeq

Department of Public Health, College of Veterinary Medicine  
University of Mosul / Mosul, Iraq

**Abstract**—Since people use internet daily they have to take care about information security requirement more and more. In this work a new algorithm for RGB based images steganography is presented. The algorithm uses LSB principle for hiding a variable number of secret message bits in RGB 24-bits color image carrier either in other one or two channels depending on the third one (index channel). The algorithm offered good capacity ratio with no visual distortion on the original image after hiding the secret message. Histograms of three channels (red, green, blue) are also compared before and after hiding process.

**Keywords**—Steganography; RGB; LSB; True color image.

## I. INTRODUCTION

Steganography is a process of hiding information. It conceals that the communication is taking place therefore when using steganography there is always secret information is being transmitted and we try to make this information not to be discovered just by the intended receiver. The sender hides a message into a cover file likes for e.g. (image, audio, video) and tries to conceal the existence of that message, later the receiver gets this cover file and detects the secret message and receives it.

Steganography which means “cover writing” it’s origin is old and backs to Golden age of Greece when people at that time had different practices to hide writing for e.g. writing on a wooden tablet and then covering it by wax, making a tattoo on a messenger head after shaving his hair and let his hair grows up again and then send him to the receiver where his hair was shaved there again to get the message. Other steganography techniques like using invisible ink for writing between lines, microdots and using character arrangement are also used [1][2][3][4].

Digital steganography has many applications in our life. When sensitive data like for e.g. ( military secrets, trade secrets, private banking information) are transmitted from source to destination they have to be protected from theft, spying, copying and claiming their ownership, as well as it could be used as a digital watermarking to protect the copyrights, also as the size of exchanged data on internet is being increased daily like store, send or receive data there must be a way to maintain availability, integrity, confidentiality and authentication of information exchanged. Steganography will solve the above problems [5][6][7].

## II. DIGITAL STEGANOGRAPHY TECHNIQUE

Digital steganography technique needs two files: the cover file; a carrier for holding the secret message and the secret message itself. A possible digital carrier can be (image, audio, video, text), this carrier will hold the secret message and seems to be an innocent file because the steganography technique hides the message and makes it detectable just by the intended receiver. The carrier together with the hidden message will produce a stego file for e.g. an image based steganography technique uses an image to hide the data then the image becomes a stego – image as illustrated in Fig.1 .

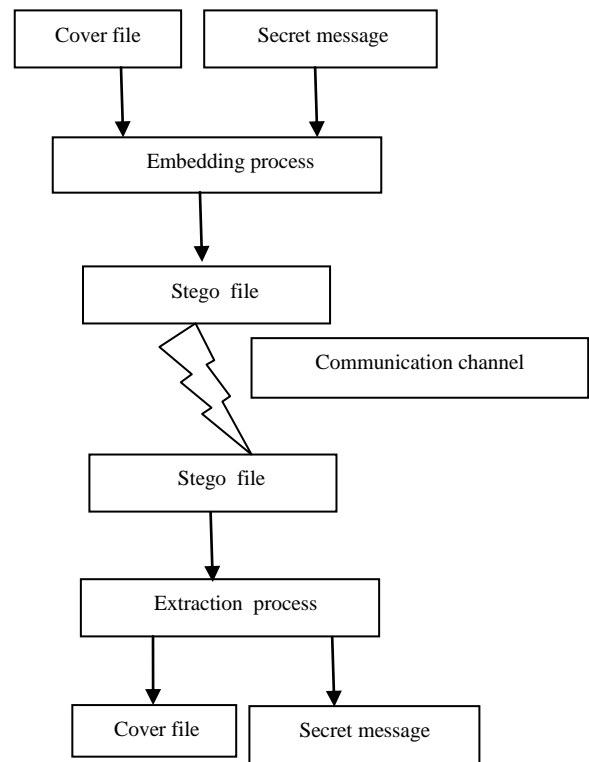


Figure (1): Basic keyless steganographic system

In image based steganography, it is desirable that a steganography technique is able to hide as many secret message bits as possible in an image in such way it will not affect the most two important requirements that are essential for hiding process and researchers take care about[8][9] :

1.Imperceptibility/security: which means that human eye cannot distinguish between the original image: (the image before hiding process) and the stego-image (the image after hiding process), in other words the hiding process cannot be detected.

2.Capacity: this term refers to the amount of data that can be embedded in a cover media.

The relationship between the above two requirements should be balanced, for e.g. if we increase the capacity more than a specified threshold value then the Imperceptibility will be affected and so on, therefore the parameters of digital steganography technique should be chosen very carefully.

### III. RGB- 24 BITS IMAGE

In this type of images, sometimes referred to as a true color image, the image is stored in computer memory as an m-by-n-by-3 array of pixels. The color of each pixel represents a combination of three components red, green and blue intensities where each component is 8 bits. This means that 16 million colors can be represented in this type of image, so RGB color space provides a wide area of colors and hiding process in this space can be more and more flexible.

### IV. LEAST SIGNIFICANT BIT INSERTION

The most common and easiest technique for data hiding is LSB (least significant bit), in this technique the effect of replacing the least significant bits of a color value with another bits will be so small that makes a difficulty by human visual system to recognize the difference between the image before and after hiding process, so the same principle is used to replace the least significant bits of a color value by hidden message bits[10][11].

#### A. An 24-bits image example:

An 24-bit image uses 3 bytes to represent a color value. (8 bits = 1 byte)

1 pixel = (00100111 11101001 11001000)  
          red        green        blue

Simplified example with a 24- bits pixel:

1 pixel: (00100111 11101001 11001000 )  
Insert 101: (00100111 11101000 11001001)  
                  red          green        blue

### V. THE PROPOSED METHOD

The proposed algorithm used true image colors (24 bits) as a carrier for a hidden message. Using of pixel indicator is presented in the proposed algorithm: two least significant bits of a channel are used as indicator of data existence in other two channels, therefore there is always an index channel and the secret data will be concealed in either one other channel or two channels depending on the value of the two LSB of index channel which is represented by K variable as illustrated in table 1. The number of secret bits that will be hidden in one channel or two channels is determined by the number calculated in bits (2, 3, and 4) of index channel which is represented by S variable in table 1. To improve security; index channel is not fixed, starting with first pixel green channel as indicator while blue is channel1 and red is channel2. In the second pixel red channel as indicator while blue is channel1 and green is channel2. In third pixel blue channel as indicator while green is channel1 and red is channel2 and so on until the hidden message bits are finished. To improve capacity; even when bits (2, 3, and 4) of the index indicate "0" or above "5" the algorithm inserts a number of hidden bits that's calculated through observation of the execution of the proposed algorithm, for e.g. green color is more effected than red and blue color when the number of hidden bits is increased, also when more than 5 bits are changed in a color value a distortion can be recognized by human visual system.

The proposed algorithm consists of two stages:

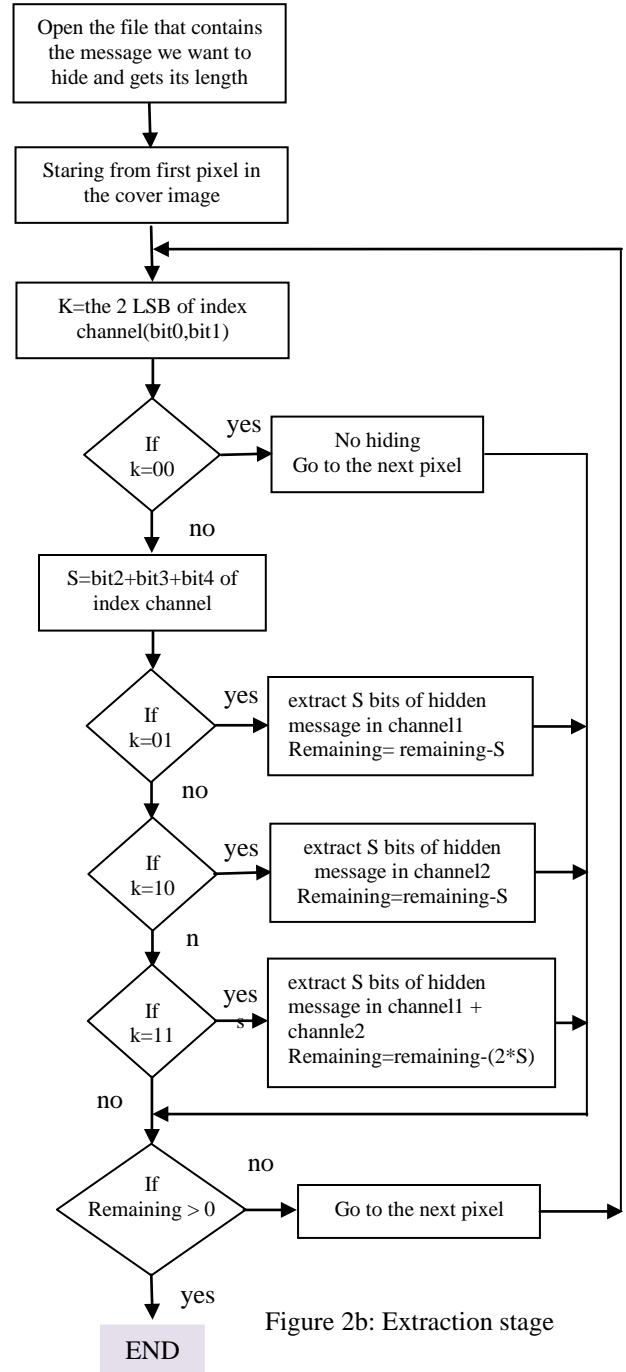
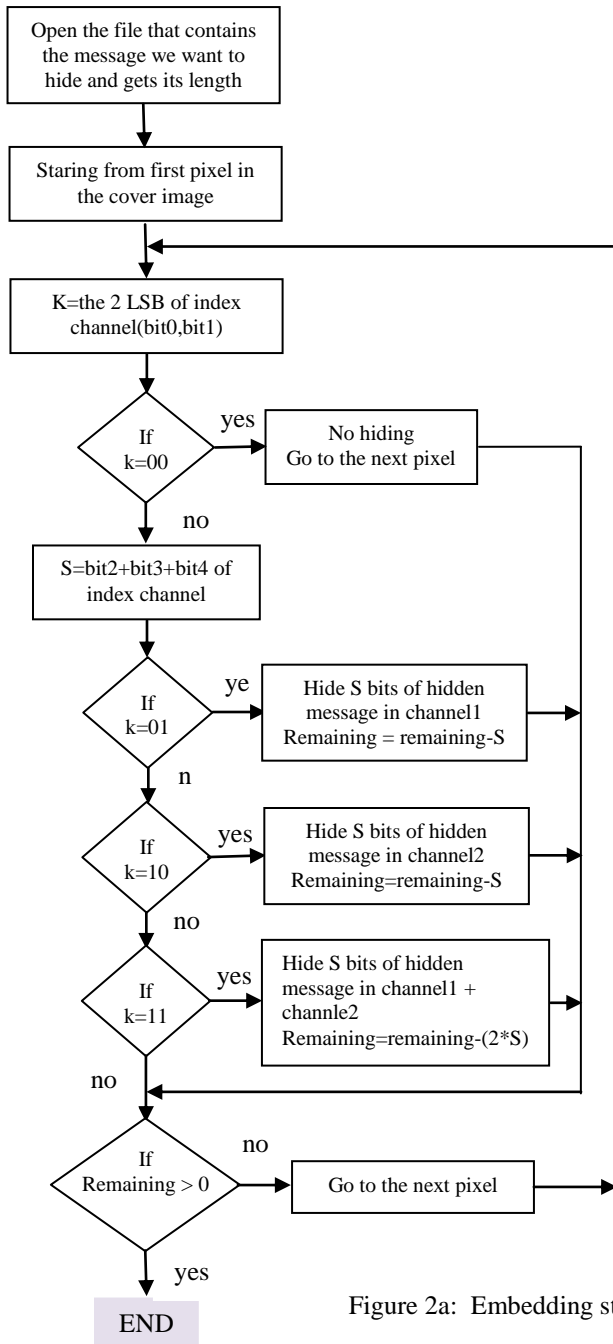
- Embedding stage.
- Extraction stage.

In stage 1 which is at the sender end the hidden bits is embedded in the cover image according to the steps of the algorithm as illustrated in Fig. 2a, and in stage 2 which is at the receiver end these hidden bits are extracted also according to the steps of the algorithm as illustrated in Fig. 2b.



TABLE 1. Meaning of index channel bits

K=bit0,bit1	Channel1	Channel2
00	No hidden bits	No hidden bits
01	hidden bits= S	No hidden bits
10	No hidden bits	hidden bits= S
11	hidden bits=S	hidden bits= S



## VI. THE RESULTS

The proposed method is presented using matlab (R2011a). A set of BMP images is chosen to do the experimentations. The images are used for hiding different length of messages. The resulting stego-images are compared with the original images there were no differences between them, as illustrated in Fig. 3 (a,b), also the histograms are generated for (R,G,B) components before and after hiding process they showed minor differences caused by the proposed algorithm as illustrated in Fig. 4 (a,b).

The experimentations show that when the length of a message becomes more than 120000 bits (i.e. 15000 characters) the resulting stego- image is still looks like the original one with no visual difference even if the length becomes 350000 bits (i.e. 43750 characters ), but from the another side the plotting of (red, green, blue ) channels of the stego-image begins to show a big difference with a comparison of the plotting of (red, green, blue ) channels of the original image.

With a comparison between the proposed algorithm and the algorithm in [12]. The results showed that the capacity ratio which is = (number of bits used each possible case)/ (total number of cases\*24) is increased from 14% in [12] to 19.2 in the proposed algorithm with no visual distortion in the stego-images. The total number of cases is 72 which decomposed as:

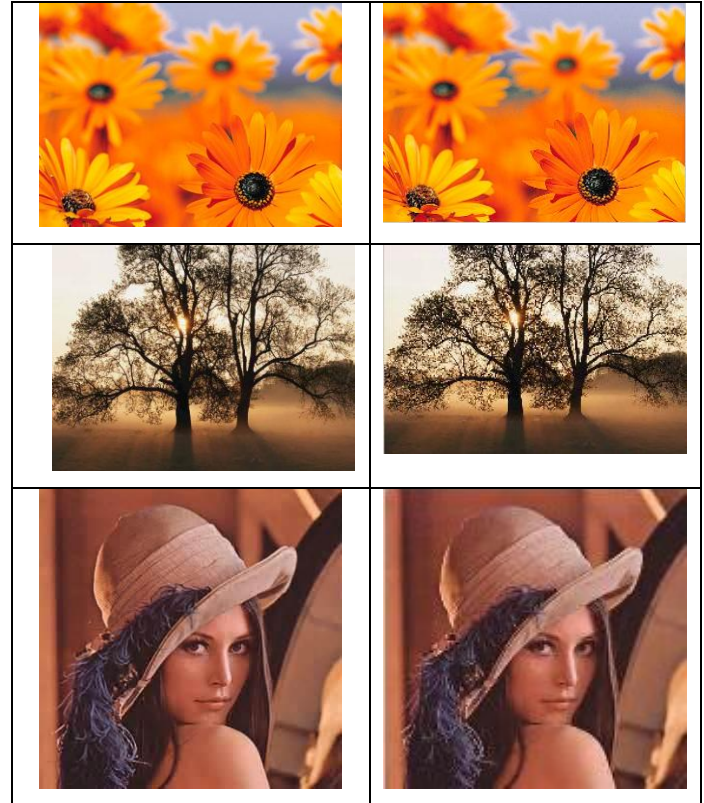
- Using one channel: we have 8 ways to determine the bits \* 6 ways to decide channel R, G or B. This results 48 cases
- Using two channels: here we have 8 ways to determine the bits\* 3 ways to determine the two channels. This results 24 cases.

Also with a comparison between the proposed method and PIT in [9], the proposed algorithm shows higher capacity ratio and better results.

Fig.4 shows the minor differences between (red, green, blue) channels before and after hiding a message of 120000 bits length (i.e. 15000 characters) for the second image (size of 512 X 384) in Fig. 3a.

Each time the message becomes longer it is hidden and retrieved correctly with all the images used without any noticed artifacts in the original images.

The proposed algorithm is tested also for hiding a binary image, the binary image is hidden without making any visual distortion and later the binary image is retrieved correctly.



(a)

(b)

Figure3: (a) original images, (b) stego-images

## VII. CONCLUSION

A new algorithm for RGB image based steganography is proposed. It uses one channel as an indicator for the existence of hidden secret message bits in the other one or two channels. The number of the inserted bits is determined by bits (2, 3, and 4) of the indicator channel.

With a comparison between the proposed algorithm and the techniques considered by this study, the proposed technique shows promising results by increasing the capacity ratio without any distortion in the stego-image.

About security enhancing, as a future work a new way for choosing the indicator is applied to add more randomization on the algorithm also encryption can be used for adding more security.

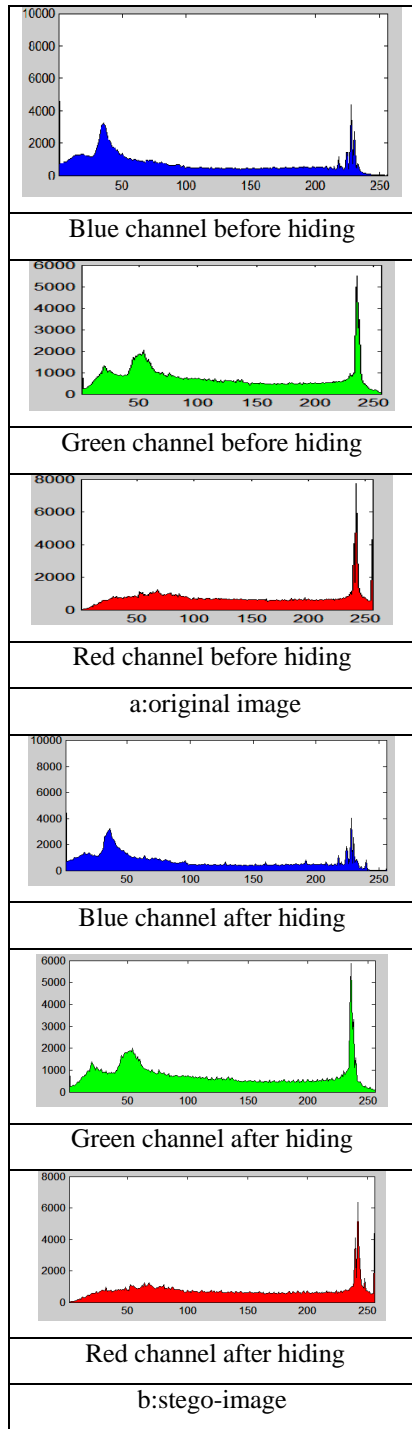


Figure4: Image steganography histograms according to proposed algorithm

## REFERENCES

- [1] Arvind Kumar, KmPooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications, Vol. 9-No.7, November 2010.
- [2] Namita Tiwaril, Madhu Shandilya, "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth", International Journal Of Security and Its Applications, Vol. 4, No. 4, October, 2010.
- [3] Walaa Abu-Marie, Adnan Gutub, Hussein Abu-Mansour, "Image Based Steganography Using Truth Table Based on Determinate Array on RGB Indicator", International Journal of Signal and Image Processing, Vol. 1-2010/Iss.3, pp. 196-204.
- [4] Ali Akbar Nikoukar, "An Image Steganography Method with High Hiding Capacity Based on RGB Image", International Journal of Signal and Image Processing, Vol. 1-2010/Iss.4, pp. 238-241.
- [5] Emad T. Khalaf, Norrozila Sulaiman,"Segmenting and Hiding Data Randomly Based on Index Channel", International Journal of Computer Science Issues, Vol. 8, Issue 3,No. 1, May 2011.
- [6] Yogendra Kumar Jain, R. R. Ahirwal, "A Novel Image Steganography Method with Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International journal of Computer Science and Security, vol. 4, issue 1.
- [7] Debnath Bhattachryya, Arpita Roy, Pranab Roy, Tai-hoon Kim, "Receiver Compatible Data Hiding Color Image", International Journal of Asvanded Scince and Technology, vol. 6, May, 2009.
- [8] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, Aleem Alvi, "Pixel Indicator High Capacity Technique for RGB Image Based Steganography", WoSPA 2008 – 5<sup>th</sup> IEEE International Workshop on Signal Processing and iys Applications, University of Sharjah, Sharjah, U.A.E 18-20 March 2008.
- [9] Adnan Abdul-Aziz Gutub, "Pixel Indicator Technique for RGB Image Steganography", Journal of Emerging Technologies in Web Intelligence, vol. 2, No. 1 Feb 2010.
- [10] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, "A Novel Steganographical Approach to Text Message Hiding In RGB Carrier Image", Journal of Basic and Applied Scientific Research, 1(12)2511-2515, 2011.
- [11] Mohammad Tanvir Parvez, Adnan Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography", 2008 IEEE Asia-Pasific Services Computing Conference.
- [12] Adnan Gutub, Ayaed Al-Qahtani, Abdulaziz Tabakh, "Triple-A: Secure RGB Image Steganography Based on Randomization", IEEE, pp. 400-403, 2009.

#### AUTHOR PROFILE

Mrs. Iman Th. Sedeeq(M. Sc) is currently a lecturer at Mosul University. She Received B.Sc. degree in Computer Science from Sciences College at Mosul University in 1993, and M.Sc. degree from Computer and Mathematics Sciences College at Mosul University in 2002. Her research interests are information security, data hiding and encryption.

# Agent Behavior in Multiagent Systems:

## Issues and Challenges in Design, Development and Implementation

Mohamed Ziyad TA

*Lecturer in Dept. of CSE  
SSM Polytechnic College  
Tirur, Kerala, INDIA*

Dr KR Shankar Kumar

*Professor in Dept. of ECE  
Sri Ramakrishna Engineering College  
Coimbatore, Tamil Nadu, INDIA*

**Abstract**—Multiagent System (MAS) technology, composed of multiple interacting intelligent agents, has become a new paradigm for modeling, designing, and implementing software solutions for complex and distributed problem solving. Multiagent system and its application have played an important part in academic research. The usages of agent based applications are increasing day by day with internet spreading widely. This study indent to address a brief area relating to the issues and challenges in the design, development and implementation of agent-based intelligent systems.

**Index Terms**—Distributed problem solving, intelligent agent, agent behavior,

### I. INTRODUCTION

Multiagent systems can be used to solve problems which are difficult or impossible for an individual agent to solve. With an overview to the computing trends, like, ubiquity, interconnection, intelligence, delegation and human-orientation required in the different phases of design and development of various systems and considering the tremendous progression in the programming paradigm have been developed from machine code and assembly language through machine independent, subroutine, procedures and functions to the most advanced objects/component oriented to agent based. There are many advantages for multiagent systems over other existing methods of application design.

- A multiagent system models serves as natural way of representing task allocation, team planning, user preferences, open environments, and so on.
- A multiagent system efficiently retrieves, filters, and globally coordinates information from sources that are spatially distributed.
- A multiagent system enhances overall system performance. It provides reliability, extensibility, robustness, maintainability, responsiveness, flexibility, and reuse.

Agents in a multiagent system are sophisticated computer programs that act autonomously on behalf of their users, across distributed environments. It can communicate via centralized agents or among themselves depending upon Design.

### II. COMPUTING CHARACTERISTICS

It is very difficult to forecast a very highly complex computing requirement and techniques that might be needed to deal with systems composed of  $10^{10}$  processors. We cannot see it as a mere “science fiction”, where as hundreds of millions of people connected by email once seemed to be so. It is assumed that the current software development models can’t handle this kind of larger and much complex scenario. Following key factors influencing the design and developmental aspects should also be taken into consideration.

#### A. Ubiquity

The continual reduction in cost of computing capability has made it possible to introduce processing power into required places and devices that would have once been uneconomic. As processing capability spreads, sophistication (and intelligence of a sort) becomes ubiquitous. What could benefit from having a processor embedded in it?

#### B. Interconnection

Computer systems today no longer stand alone, but are networked into large distributed systems. The internet is an obvious example, but networking is spreading its ever-growing tentacles. Since distributed and concurrent systems have become the norm, some researchers are putting forward theoretical models that portray computing as primarily a process of interaction.

#### C. Intelligence

The complexity of tasks that we are capable of automating and delegating to computers has grown steadily. If you don’t feel comfortable with this definition of “intelligence”, it’s probably because you are a human.

#### D. Delegation

Computers are doing more for us, without our intervention. We are giving control to computers, even in safety critical tasks. One example: fly-by-wire aircraft, where the machine’s judgment may be trusted more than an experienced pilot. Next on the agenda: fly-by-wire cars, intelligent braking systems, cruise control that maintains distance from car in front, etc.

### E. Human Orientation

The movement away from machine-oriented views of programming toward concepts and metaphors that more closely reflect the way we ourselves understand the world. Programmers (and users!) relate to the machine differently. Programmers conceptualize and implement software in terms of higher-level more human-oriented abstractions.

### III. MULTIAGENT REVOLUTION

Delegation and Intelligence imply the need to build computer systems that can act effectively on our behalf. This implies: The ability of computer systems to act *independently* or The ability of computer systems to act in a way that *represents our best interests* while interacting with other humans or systems.

Interconnection and Distribution have become core motifs in Computer Science. But Interconnection and Distribution, coupled with the need for systems to represent our best interests, implies systems that can *cooperate* and *reach agreements* (or even *compete*) with other systems that have different interests (much as we do with other people).

These issues were not studied in Computer Science until recently. All of these trends have led to the emergence of a new field in Computer Science: “*multiagent systems*”.

### IV. DEFINITION OF AGENT

An agent is a computer system that is capable of *independent* action on behalf of its user or owner (figuring out what needs to be done to satisfy design objectives, rather than constantly being told).

A multiagent system is one that consists of a number of agents, which *interact* with one-another. In the most general case, agents will be acting on behalf of users with different goals and motivations. To successfully interact, they will require the ability to *cooperate*, *coordinate*, and *negotiate* with each other, much as people do.

This study address two key problems:

a) *How do we build agents capable of independent, autonomous action, so that they can successfully carry out tasks we delegate to them?*

b) *How do we build agents that are capable of interacting (cooperating, coordinating, negotiating) with other agents in order to successfully carry out those delegated tasks, especially when the other agents cannot be assumed to share the same interests/goals?*

The first problem is agent design (micro), the second is society design (macro). The Design phase of a multiagent system will arouse the following questions such as:

- How can cooperation emerge in societies of self interested agents?
- What kinds of languages can agents use to communicate?
- How can self-interested agents recognize conflict, and how can they (nevertheless) reach agreement?
- How can autonomous agents coordinate their activities so as to cooperatively achieve goals?

While these questions are all addressed in part by other disciplines (notably economics and social sciences), what makes the multiagent systems field unique is that it emphasizes that the agents in question are *computational, information processing* entities.

### V. AMBIGUITIES IN AGENT PARADIGM

Multiagent Systems design and definition of agent behavior will need to address many uncertainties like:

1) *How can cooperation emerge in societies of self interested agents?*

2) *What kinds of languages can agents use to communicate?*

3) *How can self-interested agents recognize conflict and how can they (nevertheless) reach agreement?*

4) *How can autonomous agents coordinate their activities so as to cooperatively achieve goals?*

While these questions are all addressed in part by other disciplines (notably economics and social sciences), what makes the multiagent systems field unique is that, it emphasizes that the agents in question are computational, information processing entities.

### VI. SCOPE AND VISION OF RESEARCH

It's easiest to understand the field of multiagent systems if you understand researchers' vision of the future.

- Fortunately, different researchers have different visions.
- The amalgamation of these visions (and research directions, and methodologies, and interests, and..) define the field.
- But the field's researchers clearly have enough in common to consider each other's work relevant to their own.

### VII. APPLICATION AREAS

#### A. Spacecraft Control

When a space probe makes its long flight from Earth to the outer planets, a ground crew is usually required to continually track its progress, and decide how to deal with unexpected eventualities. This is costly and, if decisions are required quickly, it is simply not practicable. For these reasons, organizations like NASA are seriously investigating the possibility of making probes more autonomous - giving them richer decision making capabilities and responsibilities. This is not fiction: NASA's DS1 has done it!

#### B. Deep Space 1

Deep Space 1 launched from Cape Canaveral on October 24, 1998. During a highly successful primary mission, it tested 12 advanced, high-risk technologies in space. In an extremely successful extended mission, it encountered comet Borrelly and returned the best images and other science data ever from a comet. During its fully successful hyper-extended mission, it conducted further technology tests. The spacecraft was retired on December 18, 2001.” – (<http://nmp.jpl.nasa.gov/ds1/>)



### C. Autonomous Agents for specialized tasks

The DS1 example is one of a generic class Agents (and their physical instantiation in robots) have a role to play in high-risk situations, unsuitable or impossible for humans. The degree of autonomy will differ depending on the situation (remote human control may be an alternative, but not always).

### D. Air Traffic Control

“A key air-traffic control system suddenly fails, leaving flights in the vicinity of the airport with no air-traffic control support. Fortunately, autonomous air-traffic control systems in nearby airports recognize the failure of their peer, and cooperate to track and deal with all affected flights”. Systems taking the initiative when necessary, Agents cooperating to solve problems beyond the capabilities of any individual agent.

### E. Internet Agents

Searching the Internet for the answer to a specific query can be a long and tedious process. So, why not allow a computer program - an agent - do searches for us? The agent would typically be given a query that would require synthesizing pieces of information from various different Internet information sources. Failure would occur when a particular resource was unavailable, (perhaps due to network failure), or where results could not be obtained.

What if the agents become better? Internet agents need not simply search. They can plan, arrange, buy, negotiate – carry out arrangements of all sorts that would normally be done by their human user. As more can be done electronically, software agents theoretically have more access To systems that affect the real-world. But new research problems arise just as quickly.

## VIII. RESEARCH ISSUES

There are many issues to be clearly addressed for the successful multiagent system design and development, like:

- How do you state your preferences to your agent?
- How can your agent compare different deals from different vendors?
- What if there are many different parameters?
- What algorithms can your agent use to negotiate with other agents ?
- What algorithms agent use to make sure you get a good deal?
- These issues aren't frivolous – automated procurement could be used massively by (for example) government agencies. The Trading Agents Competition is also to be addressed.

Multiagent Systems is Interdisciplinary. The field of Multiagent Systems is influenced and inspired by many other fields, like: Economics, Philosophy, Game Theory, Logic, Ecology, Social Sciences, etc. This can be both a strength (infusing well-founded methodologies into the field) and a weakness (there are many different views as to what the field is about) This has analogies with artificial intelligence itself.

## IX. GENERAL VIEWS ON MULTIAGENT SYSTEMS

*a) Agents as a paradigm for software engineering: Software engineers have derived a progressively better understanding of the characteristics of complexity in software. It is now widely recognized that interaction is probably the most important single characteristic of complex software.*

*b) Over the last two decades, a major Computer Science research topic has been the development of tools and techniques to model, understand, and implement systems in which interaction is the norm.*

*c) Agents as a tool for understanding human societies: Multiagent systems provide a novel new tool for simulating societies, which may help shed some light on various kinds of social processes.*

*d) This has analogies with the interest in “theories of the mind” explored by some artificial intelligence researchers.*

*e) Multiagent Systems is primarily a search for appropriate theoretical foundations: We want to build systems of interacting, autonomous agents, but we don't yet know what these systems should look like.*

*f) You can take a “neat” or “scruffy” approach to the problem, seeing it as a problem of theory or a problem of engineering.*

*g) This, too, has analogies with artificial intelligence research.*

## X. CHALLENGES

There are many challenges taken into account for the initially study and design aspect concerning to design and implementation of a multiagent system with intelligent agents. A few of them are listed with respective other options.

### 1) Isn't it all just Distributed/Concurrent Systems?

*a) There is much to learn from this community, but: Agents are assumed to be autonomous, capable of making independent decision – so they need mechanisms to synchronize and coordinate their activities at run time.*

*b) Agents are (can be) self-interested, so their interactions are “economic” encounters.*

### 2) Isn't it all just AI?

*a) We don't need to solve all the problems of artificial intelligence (i.e., all the components of intelligence) in order to build really useful agents.*

*b) Classical AI ignored social aspects of agency. These are important parts of intelligent activity in real-world settings.*

### 3) Isn't it all just Economics/Game Theory?

*a) These fields also have a lot to teach us in multiagent systems, but: Insofar as game theory provides descriptive concepts, it doesn't always tell us how to compute solutions; we're concerned with computational, resource-bounded agents.*



*b) Some assumptions in economics/game theory (such as a rational agent) may not be valid or useful in building artificial agents.*

*4) Isn't it all just Social Science?*

*a) We can draw insights from the study of human societies, but there is no particular reason to believe that artificial societies will be constructed in the same way.*

*b) Again, we have inspiration and cross fertilization, but hardly subsumption.*

## XI. CONCLUSION

The agents in a multi-agent system have several important characteristics

- Autonomy: the agents are at least partially autonomous
- Local views: no agent has a full global view of the system, or the system is too complex for an agent to make practical use of such knowledge.
- Decentralization: there is no one controlling the whole system (or the system is effectively reduced to a monolithic system).

Intelligent agents in a multiagent environment can props, refuse or accept an offer and counter offer and try to obtain a mutually beneficial agreement as a negotiation's result.

A lot of research has been done in the field of multi agent systems which mainly concerned following areas:

*a) Developing Autonomous Agents : Many researchers have been working on how to model a system as a multi agent system which helps them in terms of: reduced modular complexity, Decentralization, adding autonomous behavior to the system, parallel execution, increased robustness etc.*

For example: in E-Commerce, we can implement autonomous agents as buyers, sellers and the auctioneers. In fact this concept has been practically adopted by some of the renowned companies like: Goldman Sachs, Amazon etc.

*b) Agent Negotiation : An increasing number of computer systems are being viewed in terms of autonomous agents. If we model them as agents, these agents will need to interact with one another, either to achieve their individual objectives or to manage the dependencies that follow from being situated in a common environment. These interactions can vary from simple information interchanges, to requests for particular actions to be performed and on to cooperation (working together to achieve a common objective) and coordination (arranging for related activities to be performed in a coherent manner). However, perhaps the most fundamental and powerful mechanism for managing inter-agent dependencies at run-time is negotiation—the process by which a group of agents come to a mutually acceptable agreement on some matter. Negotiation underpins attempts to cooperate and coordinate (both between artificial and human agents) and is required both when the agents are self interested and when they are cooperative. It is so central precisely because the agents are autonomous. When building an autonomous agent which is capable of flexible and sophisticated negotiation, the main questions that should be*

*considered are: (i) what negotiation protocol will be used? (ii) what reasoning model, decision making procedures and strategies will the agents employ?*

*c) Agent Communication : In multiagent system how the agents can communicate with other agents. The important issues here are: (i) The language in which the communications are made (ii) Communication protocols used.*

Some of the major application areas are:

- Agent based auction systems : One of the auctions techniques usually used in the agent based ecommerce is the English Auctions. In multi-agent based auction system agent's interaction or negotiation can be done in two ways (1) Through Centralized Agent (2) Negotiation with each other
- Agents in Bioinformatics : The kinds of resources available in the bioinformatics domain, with numerous databases and analysis tools independently administered in geographically distinct locations, lend themselves almost ideally to the adoption of a multi-agent approach. Here, the environment is open, distributed and dynamic, with resources entering and leaving the system over time. There are likely to be large numbers of interactions between entities for various purposes, and the need for automation for automation is substantial and pressing.

## REFERENCES

- [1] Sarit Kraus, Strategic Negotiation in Multi agent Environment MIT press 2001.
- [2] Michel Wooldridge, An introduction to Multi agent Systems, Wiley 2000
- [3] Russel, Norvig, Artificial Intelligence : A modern Approach, Pearson education 2003
- [4] Sarit Kraus Automated Negotiation and Decision Making in Multiagent Environments ACAI 2001, LNAI 2086, pp. 150–172, 2001.
- [5] Springer-Verlag Berlin Heidelberg 2000
- [6] Jennings N. An agent-based approach for building complex software systems. Communications of the ACM 2001;44:35–41.
- [7] Wooldridge M, Jennings N. Agent theories, architectures and languages: a survey. In: Intelligent Agents, ECAI-94 Workshop on AgentTheories, Architectures and Languages. Amsterdam.
- [8] Jennings N, Wooldridge M. Applications of intelligent agents. In: Agent Technology: Foundations, Applications, and Markets. New York: Springer-Verlag, 1998
- [9] Finin T, Fritzson R, McKay D, McEntire R. KQML as an Agent Communication Language. In: Proceedings of the 3<sup>rd</sup> International Conference on Information and Knowledge Management. Maryland, United States: ACM Press, 1994:pp. 456–63.

# A Comparative Study of VoIP Protocols

Hadeel Saleh Haj Aliwi, Putra Sumari  
Multimedia Computing Research Group  
School of Computer Sciences  
Universiti Sains Malaysia  
Penang, Malaysia

**Abstract**— Nowadays, Multimedia Communication has been developed and improved rapidly in order to enable users to communicate between each other over the Internet. In general, the multimedia communication consists of audio, video and instant messages communication. This paper surveys the functions and the privileges of different voice over Internet protocols (VoIP), such as InterAsterisk eXchange Protocol (IAX), Session Initiation Protocol (SIP), and H.323 protocol. As well as, this paper will make some comparisons among them in terms of signaling messages, codec's, transport protocols, and media transport, etc.

**Keywords**- *Multimedia; VoIP; InterAsterisk eXchange Protocol (IAX); Session Initiation Protocol (SIP); H.323 protocol; Signaling Messages*

## I. INTRODUCTION

Over the last few years, the needs to provide the communication facilities among participants everywhere and every time via computer network systems have been increased. These network systems enable the use of multimedia applications with many kinds of media data, such as audio, video, graphics, images, and text. This rapid expansion and potential underlies the significance of the interworking. Multimedia technology promises to make smooth and very effective interactions among people in different geographical areas [18]. However, the provided multimedia services must be improved.

In recent years, Voice over IP (VoIP) technologies [15] has been developed and many significant progresses have been done in research and commercially. VoIP allows many users to make VoIP phone calls instead of the Public Switched Telephone Network (PSTN) through such technologies as InterAsterisk eXchange Protocol (IAX) [1][5], Session Initiation Protocol (SIP) [12], and H.323 protocol [25][26]. VoIP can offer a higher quality and yet more reasonable phone service than PSTN. The telecommunication industry is going towards using VoIP as their main phone infrastructure [15]. VoIP services become so popular in the last few years because it is inexpensive compared to the traditional telephony. VoIP can be integrated with other services, such as video conferences, instant messages and presence services.

Several signaling protocols and techniques are used to help bridging the gap between the endpoints, such as H.323 Protocol, SIP protocol [16], IAX protocol, etc. These protocols provide video, audio, and data communication among participants [17]. In order to provide media transfer between participants, the signaling messages of each protocol are discussed in this paper.

This paper is organized into 4 sections; **II** briefly describes the privileges of VoIP protocols and compares among their own signals. **III** is the first comparison of VoIP protocols in term of media codec's. **IV** is the second comparison of VoIP protocols in terms of transport protocols, media transport, and others. And **V** is a summary of this paper and our planned future research.

## II. VOIP PROTOCOLS

### A. Session Initiation Protocol (SIP)

SIP is an application-layer control protocol [11] that can establish, modify, and terminate multimedia sessions (conferences) such as Internet telephony calls [9][14][25][26][27]. SIP can also invite participants to already existing sessions, such as multicast conferences. Media can be added to (and removed from) an existing session. SIP transparently supports name mapping and redirection services, which supports personal mobility-users can maintain a single externally visible identifier regardless of their network location [12][13]. SIP protocol enables Internet endpoints (called user agents) to discover one another and to agree on a characterization of a session they would like to share. For locating prospective session participants, and for other functions, SIP enables the creation of an infrastructure of network hosts (called proxy servers) to which user agents can send registrations, invitations to sessions, and other requests. SIP is an agile, general-purpose tool for creating, modifying, and terminating sessions that works independently of underlying transport protocols and without dependency on the type of session that is being established [19][20][22][23][28].

SIP does not carry any voice or video data itself. It merely allows two endpoints to set up connection to transfer

that traffic between each other via Real-time Transport Protocol (RTP) [3][15]. The User Datagram Protocol (UDP) and Transport Control Protocol (TCP) [2] are transport protocols used to transfer audio and video data [4]. SIP protocol has many features such as the service of text-based which allows easy implementation in object oriented programming languages, flexibility, extensibility, less signaling, transport layer-protocol neutral and parallel search [22][23][24]. SIP uses many signaling messages in order to handle the communication between two nodes or more. Figure 1 shows the SIP call setup between two nodes.

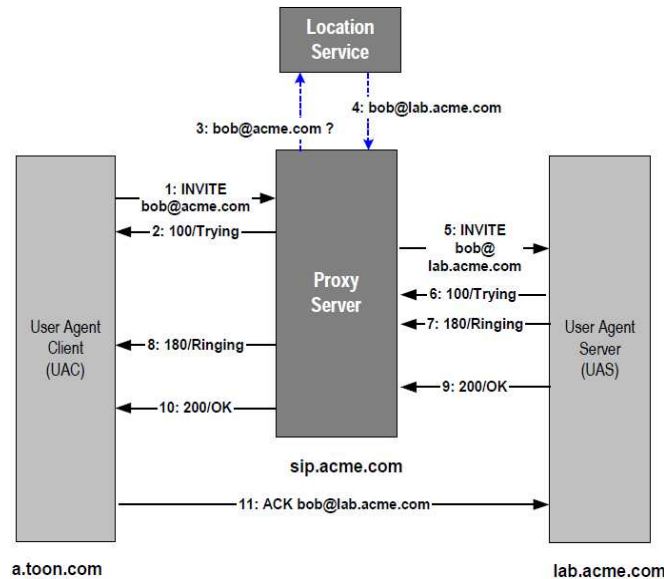


Figure 1. Call Setup with SIP [10]

SIP makes use of the six request methods: INVITE, ACK, OPTIONS, BYE, CANCEL and REGISTER in order to control the registration, call setup, and call teardown [25]. Table I describes the request messages in details.

TABLE I. SIP REQUEST METHODS [25]

SIP Request Messages	Usage
INVITE	To invite a user to participate in a multimedia session
ACK	To confirm that the final response has received
OPTIONS	To query the server capabilities.
BYE	To leave the call session
CANCEL	To abort a previous request
REGISTER	To inform the registrar of the client's current location

SIP requests are followed by one or more SIP responses, which are classified into six categories [25]. Table II shows the SIP response messages.

TABLE II. SIP RESPONSE METHODS [25]

SIP Response Messages	Usage
1xx Informational	Request received, continuing to process request
2xx Success	The action was successfully received
3xx Redirection	Further action must be taken to complete the request
4xx Client Error	The request contains bad syntax or cannot be fulfilled at this server
5xx Server Error	The request cannot be fulfilled at this server because of server error
6xx Global Failure	The request is invalid at any server

#### B. InterAsterisk eXchange Protocol (IAX)

In (2004) Mark Spencer [5] has created the Inter-Asterisk eXchange (IAX) protocol for asterisk that performs VoIP signaling [6][7]. Streaming media is managed, controlled and transmitted through the Internet Protocol (IP) networks based on this protocol. Any type of streaming media could be used by this protocol. However, IP voice calls are basically being controlled by IAX protocol [14]. Furthermore, this protocol can be called as a peer to peer (P2P) protocol that performs two types of connections which are Voice over IP (VoIP) connections through the servers and Client-Server communication. IAX is currently changed to IAX2 which is the second version of the IAX protocol. The IAX2 has deprecated the original IAX protocol [5]. Call signaling and multimedia transport functions are supported by the IAX protocol. In the same session and by using IAX, Voice streams (multimedia and signaling) are conveyed. Furthermore, IAX supports the trunk connections concept for numerous calls. The bandwidth usage is reduced when this concept is being used because all the protocol overhead is shared for all the calls between two IAX nodes. Over a single link, IAX provides multiplexing channels [11].

IAX is a simple protocol in such a way Network Address Translation (NAT) traversal complications are avoided by it [8]. The Mini and Full frames are sent between two endpoints A and B. Each audio/video flow is of IAX Mini

Frames (M frames) which contains 4 byte header. The flow is supplemented by periodic Full Frames (F Frames) includes synchronization information. User Datagram Protocol (UDP) is a transport protocol used by IAX to transfer audio and video data [4]. Figure 2 shows the ongoing call between two IAX endpoints.

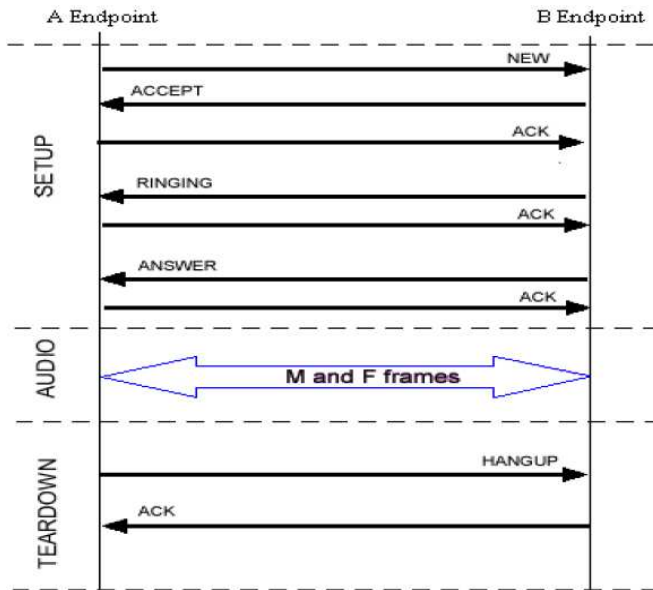


Figure 2. IAX Communication [7]

IAX uses several signals (i.e. NEW, RINGING, ANSWER, HANGUP, etc) in order to setup or teardown the call between two clients [8]. Table III explains the functions of IAX signaling methods.

TABLE III. IAX SIGNALING MESSAGES [8]

IAX Signals	Usage
NEW	To place calls
AUTHREQ	To authenticate
ACCEPT	To accept call leg
PROCEEDING	Proceed to join
RINGING	Ring at destination
ANSWER	In Call
ACK	Acknowledgment
HANGUP	To end the call

### C. H.323 Protocol

H.323 is an umbrella standard that provides well-defined system architecture [10], and implementation guidelines that cover call set-up, call control, and the media used in the call [24][25][26]. It was established by the International Telecommunications Union (ITU) as the first communications protocol for real time multimedia communication over IP. H.323 takes the more telecommunications-oriented approach to voice/video over IP. H.323 protocol provides a comparable functionality using different mechanisms and offers highly network management and interoperability [21][27].

H.323 protocol uses either TCP or UDP to transmit the audio/video packet to the destination side. As well as, Real time Transport protocol (RTP) is used to carry the media packets via Internet. Figure 3 Shows how does H.323 set up the call between to nodes.

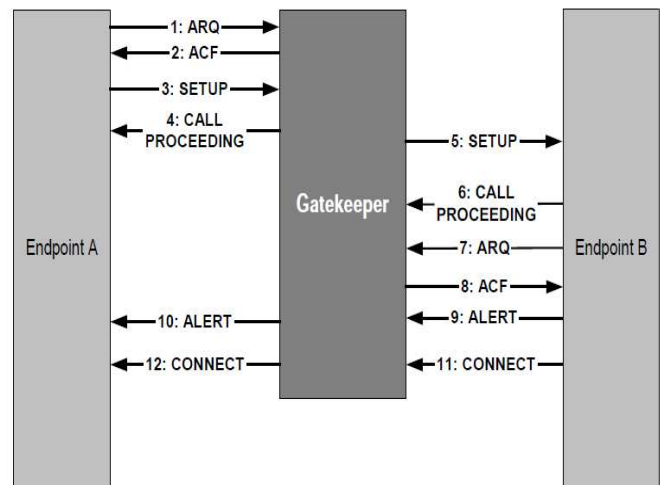


Figure 3. Call Setup with H.323 [10]

H.323 protocol has many signals used to manage and control the call, such as ARQ, ACF, ALERT, etc. Some of these messages are used to confirm, reject, and request the messages [29]. Table IV illustrates the H.323 signals.

TABLE IV. H.323 SIGNALING MESSAGES [29]

H.323 Signals	Usage
Setup	To initially request that a call is set up
Call Proceeding	To indicate that the call has is currently being processed by the called terminal
Alert	The called terminal is ringing

ARQ	Admission request
Connect	The two-way communication is ready to commence
Reject	A rejection message is sent and call setup is halted.
Release Complete	An indication that the sender wishes to end the call
ACF	Admission Confirm Message

### III. THE CODEC'S USED IN VOIP PROTOCOLS

In this section, we will compare between IAX, SIP, and H.323 in terms of codec's used for each of them [7][30]. Table V shows the comparison of the three VoIP protocols.

TABLE V. MEDIA CODEC'S OF IAX, SIP, AND H.323

	IAX	SIP	H.323
G.711	√	√	√
G.721	√	×	×
G.722	√	√	√
G.723	√	√	√
G.726	√	×	√
G.728	×	√	√
G.729	√	√	√
GSM	√	√	×
Speex	√	√	√
iLBC	√	√	×
ACC	×	√	√
AAL2	√	×	×
IMA ADPCM	√	×	×
LPC10	√	×	×
T.140	×	×	√
H.261	×	×	√
H.263	×	√	√
H.264	√	√	√

### IV. TRANSPORT PROTOCOLS, MEDIA TRANSPORT, SERVER NEEDED, IP PORTS, CALL SETUP SIGNALS, AND HEADERS USED IN VOIP PROTOCOLS

In this section, we will do another comparison of IAX, SIP, and H.323 in terms of transport protocol, media transport, call setup signals, etc [1][30]. Table VI shows the comparison of the three VoIP protocols.

TABLE VI. A COMPARISON AMONG IAX, SIP, AND H.323

	IAX	SIP	H.323
<b>Transport Protocol</b>	UDP	TCP, UDP	TCP, UDP
<b>Media Transport</b>	Full/Mini Frames	RTP/RTCP, SRTP	RTP/RTCP, SRTP
<b>Server Needed</b>	Peer to peer	Proxy Server	Gatekeeper
<b>IP Port for TCP/UDP</b>	4569	5060	3230-3253 5001 5004-6004
<b>Call Setup</b>	New→ ←Accept Ack→	Invite→ ←200Ok Ack→	Setup→ ←Connect Ack→
<b>Header Used</b>	Full/Mini Headers	RTP Header	RTP Header

### V. CONCLUSION

This paper surveys the functions and the privileges of different VoIP protocols (i.e. IAX, SIP, and H.323). In this paper, we made some comparisons of these protocols in terms of request/response signals, media codec's used, transport protocols, media transport, etc. We can observe that each protocol has its own privileges that differ from the others. In the future, we will do another comparison in terms of quality of services (packet delay, packet loss, jitter, and packet reordering), bandwidth consumption, services, extensibility, scalability, etc.

### REFERENCES

- [1] H. S. Haj Aliwi, S. A. Alomari, and P. Sumari, "An Effective Method For Audio Translation between IAX and RSW Protocols," World Academy of Science, Engineering and Technology 59 2011, pp.253-256, 2011.
- [2] A. S. Tanenbaum, "Computer Networks," 4<sup>th</sup> edition, Pearson Education, Inc, 2003.
- [3] C. Perkins, "RTP: Audio and Video for the Internet," Addison Wesley, USA, 2003.
- [4] D. DiNicolo, "Transporting VoIP Traffic with UDP and RTP," 2007.
- [5] M. Spencer, and F. W. Miller, "IAX Protocol Description," 2004.

- [6] M. S. Kolhar, A. F. Bayan, T.C. Wan, O. Abouabdalla, and S. Ramadass, "Control and Media Session: IAX with RSW Control Criteria," Proceedings of International Conference on Network Applications, Protocols and Services, Executive Development Centre, Universiti Utara Malaysia, pp. 130-135, 2008.
- [7] M. S. Kolhar, A. F. Bayan, T.C. Wan, O. Abouabdalla, and S. Ramadass, "Multimedia Communication: RSW Control Protocol and IAX," The 5th International Symposium on High Capacity Optical Networks and Enabling Technologies, Penang, Malaysia, pp. 75-79, 2008.
- [8] M.S. Kolhar, M.M. Abu-Alhaj, O. Abouabdalla, T.C. Wan, and A. M. Manasrah, "Comparative Evaluation and Analysis of IAX and RSW," International Journal of Computer Science and Information Security, pp. 250-252, 2009.
- [9] O. Abouabdalla, and S. Ramadass, "Enable Communication between the RSW Control Criteria and SIP Using R2SP," The 2nd International Conference on Distributed Frameworks for Multimedia Applications, pp. 1-7, 2006.
- [10] Radvision, "Overview of H.323-SIP interworking," © 2001 RADVISION Ltd, [www.radvision.com/NR/.../Overview of H323SIPInterworking.pdf](http://www.radvision.com/NR/.../Overview%20of%20H323SIPInterworking.pdf) (last accessed March 25, 2012), 2001.
- [11] P. Montoro, and E. Casilari, "A Comparative Study of VoIP Standards with Asterisk," Proceedings of the 2009 Fourth International Conference on Digital Telecommunications, pp. 1-6.
- [12] M. Handley, H. Schulzrinne, and E. Schooler, "SIP: session initiation protocol," Internet Draft, Internet Engineering Task Force, <http://www.ietf.org/rfc/rfc3261.txt> (last accessed Sep 25, 2011), 1998.
- [13] M. F. EESSA, "Instant Messaging Interoperability Module between the Session Initiation Protocol (SIP) and the Multipoint File Transfer System (MFTS)," Master Thesis, USM, Penang, Malaysia, 2009.
- [14] T. Abbasi, S. Prasad, N. Seddigh, and Ioannis Lambadaris, "A Comparative Study of the SIP and IAX," Canadian Conference on Electrical and Computer Engineering, pp. 179- 183, 2005.
- [15] M. Adams & M. Kwon, "Vulnerabilities of the Real-Time Transport (RTP) Protocol for Voice over IP (VoIP) Traffic," Proceedings of the 6th IEEE Conference on Consumer Communications and Networking Conference, USA, pp.958-962, 2009.
- [16] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinouidakis, and S. Gritzalis, "Survey of security vulnerabilities in session initiation protocol," Communications Surveys & Tutorials, IEEE, pp. 68-81, 2006.
- [17] S. Ramadass and R. K. Subramaniam, "A control criteria to optimize collaborative document and multimedia conferencing bandwidth requirements," In Proceedings of IEEE Singapore International Conference on 'Electrotechnology 2000: Communications and Networks', Singapore, pp. 555-559, 1995.
- [18] S. Ramadass, "A distributed architecture to support multimedia applications over the internet and corporate intranets," In proceedings of SEACOMM'98, Penang, Malaysia, 1998.
- [19] A. Toufik, M. Ahmed, and B. Raouf, "Interworking between sip and mpeg-4 dmif for heterogeneous ip video conferencing," Proc. of the IEEE ICC, vol.25, no.1, pp. 2469-2473, Apr. 2002.
- [20] M.F Aboalmaaly, O.A. Abouabdalla, H. A. Albaroodi, and A.M. Manasrah, "Point-to-Point IM Interworking Session Between SIP and MFTS," (IJCSIS) International Journal of Computer Science and Information Security, pp. 84-87, 2010.
- [21] L. Wang, A. Agarwal, and J. W. Atwood, "Modeling and verification of interworking between sip and h.323," In Proceedings of Computer Networks, pp. 77 - 98, 2004.
- [22] M. Baklizi, N. Abdullah, O. Abouabdalla, and S. Ahmadpour, "SIP and RSW: A Comparative Evaluation Study," International Journal of Computer Science and Information Security, pp. 117-119, 2010.
- [23] Y. Zhang, "SIP-based VoIP network and its interworking with the PSTN," Electronics & Communication Engineering Journal, pp. 273-282, 2002.
- [24] I. Dalgic and H. Fang, "Comparison of H.323 and SIP for IP Telephony Signaling," in Proc. of Photonics East, (Boston, Massachusetts), SPIE, 1999.
- [25] P. Papageorgiou, "A Comparison of H.323 vs SIP," Master Thesis, University of Maryland at College Park, USA, 2001.
- [26] H. Schulzrinne and J. Rosenberg, "A Comparison of SIP and H.323 for Internet Telephony," In Proceedings of the 8th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV'98), Cambridge, UK, pp. 83-86, 1998.
- [27] N. Networks, "A Comparison of H.323v4 and SIP," Technical Report, 3GPP S2, Japan, S2-000505, <http://www.cs.columbia.edu/sip/papers.html>, (Last accessed Sep 20, 2011), 2000.
- [28] A. B. Johnston, "SIP: Understanding the Session Initiation Protocol," Artech House, 2001.
- [29] Voice over IP Calculator, "H.323 Primer", free VoIP technical resources, <http://www.voip-calculator.com/h323primer.html>, (Last accessed May, 25, 2012), 2007.
- [30] Cisco Technical Help, "H.323 versus SIP: A Comparison", <http://cisco-information.blogspot.com/2007/09/h323-versus-sip-comparison.html>, (Last accessed May, 25, 2012), September, 1, 2007.



**Hadeel Saleh Haj Aliwi** has obtained her Bachelor degree in Computer Engineering from Ittihad Private University, Syria in 2007-2008 and Master degree in Computer Science from Universiti Sains Malaysia, Penang, Malaysia in 2011. Currently, she is a PhD candidate at the School of Computer Science, Universiti Sains Malaysia. Her main research area

interests are in includes Multimedia Networking, VoIP protocols, Interworking between Heterogeneous protocols, and Instant Messaging protocols.



**Putra Sumari** obtained his MSc and PhD in 1997 and 2000 from Liverpool University, England. Currently, he is Associate Professor and a lecturer at the School of Computer Science, USM. He is the head of the Multimedia Computing Research Group, CS, USM. Member of ACM and IEEE, Program

Committee and reviewer of several International Conference on Information and Communication Technology (ICT), Committee of Malaysian ISO Standard Working Group on Software Engineering Practice, Chairman of Industrial Training Program, School of Computer Science, USM, Advisor of Master in Multimedia Education Program, UPSI, Perak.



# A Novel Approach For Object Detection and Tracking using IFL Algorithm

R.Revathi

Research Scholar, Dept. of Computer Science  
Karpagam University  
Coimbatore, India

M.Hemalatha

Dept. of Computer Science  
Karpagam University  
Coimbatore, India

**Abstract**—This paper is an innovative attempt has been made using Attanassov's Intuitionistic fuzzy set theory for tracking moving objects in video. The main focus of this proposed work is taking an account for handling uncertainty in assignment of membership degree known as hesitation degree using Intuitionistic fuzzy. Many algorithms have been developed to reduce the computational complexity of movement vector evaluation. In this paper we propose to implement Intuitionistic logic based block Matching Algorithm termed as BMIFL to overcome the computational complexity. In this proposed methodology feature extraction is performed using 2D filter, segmentation using approximate median and object detection is done using our proposed algorithm Intuitionistic fuzzy. The results obtained clearly shows that our algorithm performs better than fuzzy logic based three Step Search algorithm

**Keywords**—component; Noise filtering, Segmentation, Object Tracking and detection, Fuzzy Logic.

## I. INTRODUCTION

**Video tracking** is the process of locating a moving object (or multiple objects) over time using a camera. It has a variety of uses, some of which are: human-computer interaction, security and surveillance, video communication and compression, augmented reality, traffic control, medical imaging [1] and video editing.<sup>[2][3]</sup> Video tracking can be a time consuming process due to the amount of data that is contained in video. Adding further to the complexity is the possible need to use object recognition techniques for tracking [4]. The association can be especially difficult when the objects are moving fast relative to the frame rate. Another situation that increases the complexity of the problem is when the tracked object changes orientation over time. [3].

## II. RELATED WORKS

Fuzzy controller system has been suggested which created a time, according to the 2 or 3 arrival parameters and their evaluation. This created time is related to the increasing of time needed when vehicles cross the junction. Shilpa et al. (2008) divided a street into 3 longitudinal traffic lanes through camera sensor and image processing. A crossing chance is provided in each lane. An operation is a function performed according to phases. Kiang and Khalid et al. (1996) simulated traffic junction on two kinds of controller system

(ordinary and fuzzy), according to cases such as waiting time, traffic density, cost etc. Barzegar et al. (2011) introduced the simulation of traffic light controller by Fuzzy Petri net through implemented operations.

An intelligent traffic light monitoring system using an adaptive associative memory was designed by Abdul Kareem and Jantan (2011). The research was motivated by the need to reduce the unnecessary long waiting times for vehicles at regular traffic lights in urban area with 'fixed cycle' protocol. To improve the traffic light configuration, the paper proposed monitoring system, which will be able to determine three street cases (empty street case, normal street case and crowded street case) by using small associative memory. The experiments presented promising results when the proposed approach was applied by using a program to monitor one intersection in Penang Island in Malaysia. The program could determine all street cases with different weather conditions depending on the stream of images, which are extracted from the streets video cameras [8]

A distributed, knowledge-based system for real-time and traffic-adaptive control of traffic signals was described by Findler and et al (1997). The system was a learning system in two processes: the first process optimized the control of steady-state traffic at a single intersection and over a network of streets while the second stage of learning dealt with predictive/reactive control in responding to sudden changes in traffic patterns [9]. GiYoung et al., (2001) believed that electro sensitive traffic lights had better efficiency than fixed preset traffic signal cycles because they were able to extend or shorten the signal cycle when the number of vehicles increases or decreases suddenly. Their work was centred on creating an optimal traffic signal using fuzzy control. Fuzzy membership function values between 0 and 1 were used to estimate the uncertain length of a vehicle, vehicle speed and width of a road and different kinds of conditions such as car type, speed, delay in starting time and the volume of cars in traffic were stored [10]. A framework for a dynamic and automatic traffic light control expert system was proposed by [11]. The model adopted inter-arrival time and inter-departure time to simulate the arrival and leaving number of cars on roads. Knowledge base system and rules were used by the model and RFID were



deployed to collect road traffic data. This model was able to make decisions that were required to control traffic at intersections depending on the traffic light data collected by the RFID reader. A paper by Tan et al., (1996) described the design and implementation of an intelligent traffic lights controller based on fuzzy logic technology. The researchers developed a software to simulate the situation of an isolated traffic junction based on this technology. Their system was highly graphical in nature, used the Windows system and allowed simulation of different traffic conditions at the junction. The system made comparisons the fuzzy logic controller and a conventional fixed-time controller; and the simulation results showed that the fuzzy logic controller had better performance and was more cost effective [12].

Research efforts in traffic engineering studies yielded the queue traffic light model in which vehicles arrive at an intersection controlled by a traffic light and form a queue. Several research efforts developed different techniques tailored towards the evaluation of the lengths of the queue in each lane on street width and the number of vehicles that are expected at a given time of day. The efficiency of the traffic light in the queue model however, was affected by the occurrence of unexpected events such as the break-down of a vehicle or road traffic accidents thereby causing disruption to the flow of vehicles. Among those techniques based on the queue model was a queue detection algorithm proposed by [13]. The algorithm consisted of motion detection and vehicle detection operations, both of which were based on extracting the edges of the scene to reduce the effects of variations in lighting conditions. A decentralized control model was described Jin & Ozguner (1999). This model was a combination of multi-destination routing and real time traffic light control based on a concept of cost-to-go to different destinations [14]. A believe that electronic traffic signal is expected to augment the traditional traffic light system in future intelligent transportation environments because it has the advantage of being easily visible to machines was propagated by Huang and Miller (2004).

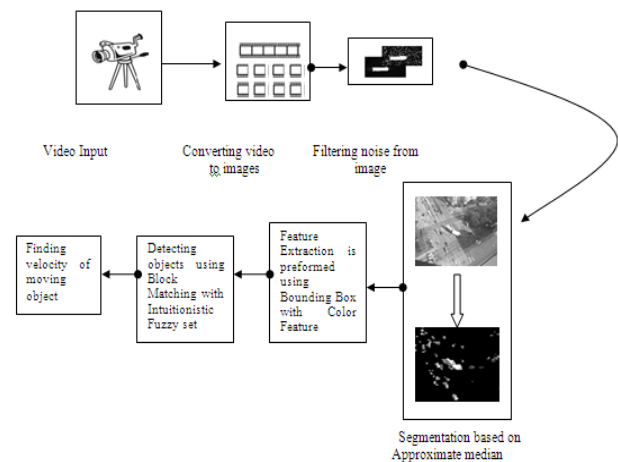
Their work presented a basic electronic traffic signaling protocol framework and two of its derivatives, a reliable protocol for intersection traffic signals and one for stop sign signals. These protocols enabled recipient vehicles to robustly differentiate the signal's designated directions despite of potential threats (confusions) caused by reflections. The authors also demonstrated how to use one of the protocols to construct a sample application: a red- light alert system and also raised the issue of potential inconsistency threats caused by the uncertainty of location system being used and discuss means to handle them [15]. Di Febraro et al (2004) showed that Petri net (PN) models can be applied to traffic control.

The researchers provided a modular representation of urban traffic systems regulated by signalized intersections and considered such systems to be composed of elementary structural components; namely, intersections and road

stretches, the movement of vehicles in the traffic network was described with a microscopic representation and was realized via timed PNs. An interesting feature of the model was the possibility of representing the offsets among different traffic light cycles as embedded in the structure of the model itself [16]. Nagel and Schreckenberg (1992) described a Cellular Automata model for traffic simulation. At each discrete time-step, vehicles increase their speed by a certain amount until they reach their maximum velocity. In case of a slower moving vehicle ahead, the speed will be decreased to avoid collision. Some randomness is introduced by adding for each vehicle a small chance of slowing down [17].

The experiences of building a traffic light controller using a simple predictor was described by Tavladaakis (1999). Measurements taken during the current cycle were used to test several possible settings for the next cycle, and the setting resulting in the least amount of queued vehicles was executed. The system was highly adaptive, however as it only uses data of one cycle and could not handle strong fluctuations in traffic flow well [18]. Chattaraj et al., (2008) proposed a novel architecture for creating Intelligent Systems for controlling road traffic. Their system was based on the principle of the use of Radio Frequency Identification (RFID) tracking of vehicles. This architecture can be used in places where RFID tagging of vehicles is compulsory and the efficiency of the system lied in the fact that it operated traffic signals based on the current situation of vehicular volume in different directions of a road crossing and not on pre-assigned times [19].

### III. OBJECT TRACKING PROPOSED METHODOLOGY



### IV. PHASES USED IN OBJECT TRACKING

#### A. Noise:

The most significant stages in image processing applications are the noise filtering. The importance of image sequence processing is regularly increasing with the ever use of digital television and video systems in consumer, commercial, medical, and communicational

applications. Image filtering is not only used to improve the image quality but also is used as a preprocessing stage in many applications including image encoding, pattern recognition, image compression and target tracking, to name a few. This preprocessing stage is essential in most of the image-processing algorithm and improper noise filtering may result in inappropriate or even false outcome. Different methods have been proposed for the purpose of noise filtering. [20].

1. Select three videos which contain three different noises like -Salt and pepper noise/ Gaussian noise /periodic noise.
2. Convert videos to Frames.
3. Apply various filters in the noise generated frames
4. Identify the best suited filter using the PSNR and MSE
5. Use the resultant frames for further processing.

From the results obtained we conclude that with three different noises salt and pepper noise, Gaussian noise and periodic noise applied for denoising of the spatial video produces variant results over different filtered techniques. From the results obtained using various filtering techniques it is observed that for salt and pepper noise median and rank order filter works better than other techniques. In case of Gaussian noise Weiner and rank order filter works fine. For Periodic noise 2D filter works better than other filters.

#### B. Segmentation:

Segmentation is the method of partitioning a digital image into multiple segments (sets of pixels, also known as super pixels). The goal of segmentation is to make simpler and/or change the representation of an image into something that is more meaningful and easier to analyze.[21] Image segmentation is characteristically used to trace objects and boundaries (lines, curves, etc.) in images.

##### 1) Approximate median segmentation

Approximate median method uses a recursive method for estimating a background model. Each pixel in the background model is compared to the corresponding pixel in the current frame, to be incremented by one if the new pixel is larger than the background pixel or decremented by one if smaller. A pixel in the background model effectively converges to a value where half of the incoming pixels are larger than and half are smaller than its value. This value is known as the median.

##### a) Process:

1. Assign the variables move to the input video, n frames to the number of frames, set the threshold value to 25 and move the frames one by one to the n (i).cdata.
2. Read the 1st background frame as bg=n(1).cdata and convert it into gray scale

3. set the frame size variables fr-size to the size of the background frame and width and height corresponding to the fr\_size.

4. convert all the frames into grayscale and type cast the operands as double to avoid negative overflow

Using  $fr\_diff = \text{abs}(\text{double}(fr\_bw) - \text{double}(bg\_bw));$

5. If fr\_diff (frame difference) of the considered frame is greater than the threshold pixel in the foreground then increment background value else decrement the background pixel value.

6. Continue step 5 for all width varying from 1 and height varying from 1.

7. Display the result using plot and imshow frame.

8. If needed save the output as movie.

#### C. Feature extraction

The feature is defined as a function of one or more measurements, each of which specifies some quantifiable property of an object, and is computed such that it quantifies some significant characteristics of the object. [22].

Feature Extraction plays a major role to detect the moving objects in sequence of frames. Every object has a specific feature like color or shape. In a sequence of frames, any one of the feature is used to detect the objects in the frame. [23]

##### 1) Bounding Box with Color Feature

If the segmentation is performed using frame difference, the residual image is visualized with rectangular bounding box with the dimensions of the object produced from residual image. For a given image, a scan is performed where the intensity values of the image are more than limit (depends on the assigned value, for accurate assign maximum). In this Features is extracted by colour and here the intensity value describes the color. The pixel values from the first hit of the intensity values from top, bottom, left and right are stored. By using this dimension values a rectangular bounding box is plotted within the limits of the values produced.[23]

##### a) Algorithm for Bounding Box:

1. Read the Image difference
2. For (pres pos=int value: final Value)of y resolution
3. For (pres pos=int value: final Value)of x resolution
  - a. Calc the sharp change in intensity of image from top and bottom
  - b. Store the values in an array
4. Height of the bounding box is = bottom value – top value
5. For (pres pos=int value: final Value)of x resolution

6. For (pres pos=int value: final Value)of y resolution
  - a. Calc the sharp change in intensity of image from left to right
  - b. Store the values in an array
7. Width of the bounding box = right value – left value
  - a. Using the Dim draw the boundary to the image .
8. Initial Value : The starting position of pixel in an image.
9. Final Value : The ending position of pixel in an image.
10. Height = Bottom value – top value/2
11. Width = Right value – Left value/2
12. Add the Height value with the top value
13. Store it in a variable like mid.top
14. Add the width value with the left value.
15. Store it in a variable like mid.left.

#### D. Object Detection

Object detection is a big part of people's lives. We, as human beings, constantly "detect" various objects such as people, buildings, and automobiles. Yet it remains a mystery how we detect objects accurately and with little apparent effort.

##### 1) Challenges in Object Detection

Automatic object detection is a difficult undertaking. In over 30 years of research in computer vision, progress has been limited. The main challenge is the amount of variation in visual appearance. An object detector must cope with both the variation within the object category and with the diversity of visual imagery that exists in the world at large.[24]

##### 2) Block Matching

A Block Matching Algorithm (BMA) is a way of locating matching blocks in a sequence of digital video frames for the purposes of motion estimation.

The purpose of a block matching algorithm is to find a matching block from a frame  $i$  in some other frame  $j$ , which may appear before or after  $i$ . This can be used to discover temporal redundancy in the video sequence, increasing the effectiveness of inter frame video compression and television standards conversion.

Block matching algorithms make use of criteria to determine whether a given block in frame  $j$  matches the search block in frame  $i$  [25]. The main advantage of block matching algorithm is the data redundancy between successive frames to reduce the storage requirements. Data compression system for quality, speed, etc.

Block matching algorithm is mainly used in Motion Estimation and Motion compression.

##### 3) Motion Estimation:

The changes between the frames are mainly due to the movement of objects using the motions of the objects between frames the encoder estimation of the motion that occurred between the reference frame and the current frame.

##### 4) Motion Compression:

The encoder uses the motion model and information to move the content of the reference frame to provide the better prediction of the current frames.

#### E. Intuitionistic Fuzzy set

The key improvement of Intuitionistic fuzzy set theory over fuzzy set theory is that in the latter, the membership value of an object also defines the non-membership value of it by means of a mathematical relation, whereas in the former the membership value and non-membership value of an object are not, in general, related by a mathematical equation. Rather, the decision-maker (or the problem analyst or the intelligent agent) independently decides both, up to his best intellectual capability. This is because, when deciding the degree of membership of an object there may be some hesitation.

A fuzzy set could be viewed as a special case of Intuitionistic fuzzy set, provided that at the processing stage for evaluation of membership value, there is no in deterministic situation with respect to any object of the universe of discourse.

An Intuitionistic fuzzy set (IFS)  $A$  on a universe  $X$  is defined as an object of the following form

$$A = \{ \langle x, \mu_A(x), \nu_A(x) \rangle \mid x \in X \}$$

Where the functions

$$\mu_A : X \rightarrow [0,1] \text{ and } \nu_A : X \rightarrow [0,1]$$

Defines the degree of membership and the degree of non-membership of the element  $x \in X$  in  $A$ , respectively and for every  $x \in X$

$$0 \leq \mu_A(x) + \nu_A(x) \leq 1$$

Obviously, each ordinary fuzzy set may be written as

$$\{ \langle x, \mu_A(x), 1 - \nu_A(x) \rangle \mid x \in X \}$$

Recently, the necessity has been stressed of taking into consideration a third parameter  $\pi_A(x)$ , known as the Intuitionistic fuzzy index or hesitation degree, which arises due to the lack of knowledge or 'personal error' in calculating the distances between two fuzzy sets [22]. In fuzzy set, non-membership value is equal to  $1 - \text{membership value}$  or the sum of membership degree and non-membership value is equal to 1. This is logically true. But in real world this may not be true as human being may not express the non-membership value as  $1 - \text{membership value}$ . This is due to the presence of uncertainty or hesitation or the lack of knowledge in defining the member ship function. This uncertainty is named as hesitation degree. Thus the summation of three degrees, i.e., membership, non-membership and hesitation degree is 1. It is obvious that  $0 \leq \pi_A(x) \leq 1$ , for each  $x \in X$ . So, with the

introduction of hesitation degree, an Intuitionistic fuzzy set A in X may be represented as

$$A = \{ \langle x, \mu_A(x), \nu_A(x), \pi_A(x) \rangle \mid x \in X \}$$

With the condition  $\mu_A(x) + \nu_A(x) + \pi_A(x) = 1$ .

#### F. PROPOSED ALGORITHM

The Three Step Search algorithm searches every one of the four side of a macro block. But occasionally the search at all the four side of a macro block is unwanted. The variation in intensity from the darker region to the lighter region or from the lighter region to the darker region is called the EDGE region of an image.

The macro block positioned on one side of edge region does not require to be searched at the other side of the edge for best match. As an example if a macro block is at the lighter side of the edge then search at the darker side of the edge is unwanted. So in this algorithm a Intuitionistic fuzzy membership value according to intensity is introduced for every macro block. Now searching the macro block of the reference frame for the best match only can continue if the Intuitionistic fuzzy degree of membership value is greater than the value of degree of non membership and degree of hesitation of that current macro block of the present frame. The search location and all other steps are similar with the conventional three step search. The proposed algorithm is similar to almost three step search and be able to be described like

1. Calculate Intuitionistic fuzzy membership value  $\mu_A(x)$ , Non membership value  $\nu_A(x)$  and hesitation value  $\pi_A(x)$  for every macro block of the reference frame.
2. Calculate Intuitionistic fuzzy membership value  $\mu_A(x)$ , Non membership value  $\nu_A(x)$  and hesitation value  $\pi_A(x)$  for every macro block of the current frame.
3. Set the search location at center and Set the Step Size  $S=4$
4. Whether the Intuitionistic fuzzy membership value of the macro block of the previous frame is greater than Non membership value  $\nu_A(x)$  and hesitation value  $\pi_A(x)$  of the macro block of the current frame.
5. Then calculate the cost function IFD for that macro block else skip the calculation.
6. The same process described in step 4 and 5 for center location is repeated for all eight locations  $\pm S$  around the center.
7. If calculation is skipped for all the nine locations then we keep the search origin same.
8. Else from these nine locations searched so far it picks the one giving least cost and makes it the new search origin.
9. According to the three step algorithm new step size is  $S=S/2$  and repeats the similar search for two more iterations until  $S=1$ .

#### G. Tracking

The process of locating the moving object in sequence of frames is known as tracking. This tracking can be performed by using the feature extraction of objects and detecting the

objects in sequence of frames. By using the position values of object in every frame, we can calculate the position and velocity of the moving object. [26][27]

#### H. Distance

The distance travelled by the object is determined by using the centroid. It is calculated by using the Euclidean distance formula. The variables for this are the pixel positions of the moving object at initial stage to the final stage. Distance measures between two Intuitionistic fuzzy sets A and B that take into account the membership degree m, the non-membership degree n, and the hesitation degree (or Intuitionistic fuzzy index) p in

$$X = \{x_1, x_2, \dots, x_n\}.$$

$$\text{Let } A = \{ \langle x, \mu_A(x), \nu_A(x) \rangle \mid x \in X \} \text{ and} \\ B = \{ \langle x, \mu_B(x), \nu_B(x) \rangle \mid x \in X \}$$

Be two Intuitionistic fuzzy sets. Considering the hesitation degree, the interval or range of the membership Degree of the two Intuitionistic fuzzy sets A and B may be represented as

$$\{(\mu_A(x), (\nu_A(x) + \pi_A(x)))\}, \{(\mu_B(x), (\nu_B(x) + \pi_B(x)))\}$$

Where

$\mu_A(x)$ ,  $\mu_B(x)$  are the membership degrees

$\nu_A(x)$ ,  $\nu_B(x)$  are the non membership degrees

$\pi_A(x)$ ,  $\pi_B(x)$  are the hesitation degrees in the respective sets, with

$$(A(x) = 1 - \mu_A(x) - \pi_A(x) \text{ and}$$

$$\pi_B(x) = 1 - \mu_B(x) - \nu_B(x).$$

The interval is due to the hesitation or the lack of knowledge in assigning membership values. The distance measure has been proposed here taking into account the hesitation degrees.

##### 1) Velocity calculation

Input: video file

Output: object detected video

Process:

1. Load the video from the avi file using video reader method and store in the variable avi.

2. Convert the pixel data in the video file into a single array using `pixels = double (cat (4, mov {1:2: end}))/255;`

3. Convert the color image into gray scale image using `rgb2gray` function and store the values in the variable `pixels`.

4. Initialize the variable `rows` and `cols` to the values such as 200,300 or 240,320 or 500,600 and names to the value of `f`.

5. Type cast the operands as double to avoid negative overflow using the function

```
d(:,l)=(abs(pixels(:,l)-pixels(:,l-1)));
```

6. for each pixel in row and cols check if the background value is greater than 0.5. if it is greater than 0.5 move that particular position to the variable `toplen`.

7. And if `cou` variable =1 then move it to `tplen` or else increment `cou` value by 1 continue step 6 for all pixels in each rows and cols.

8. Format the output and display the results as labelled image , measurements and bounding box with a particular height and width.

## V. EXPERIMENTAL RESULT

The experimental results are conducted with the help of MATLAB R2007a. Intel® Core™2DUO CPU T5870 and speed 2.00 GHZ and its capacity are 2.99GB of RAM. The proposed framework act of the object tracking is achieved by four stages and they are discussed below

### A. Noise Removal Technique

The input video may suffer from noises due to three main reasons are as follows:

- Light level and sensor temperature
- Atmospheric disturbance during transmission
- The imaging equipment which is subject to electronic disturbance of a repeating nature.

Prior to any other processing phase the input video has to be preprocessed to remove the noises to increase the quality of video as well as increase the efficiency of object tracking

In this Preprocessing stage the video with Gaussian noise, salt and pepper noise and Periodic Noise are taken under consideration. The test was conducted on these videos by applying different noise filters. The result shows for Gaussian noise the wiener filter best suits, Salt and Pepper noise is effectively removed by Median filter and for the periodic noise 2D FIR filter performs better than other filters. The result obtained are shown in the below figures

Gaussian noise

Wiener Filter



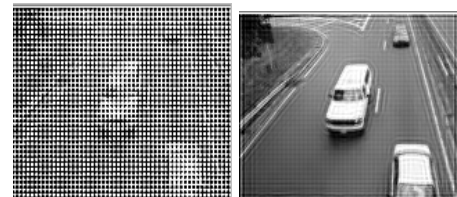
Salt And Pepper Noise

Median Filter



Periodic Noise

2D FIR Filter



### B. Segmentation Technique

The segmentation technique is used to cluster the related objects by performing background subtraction using Average Median.

Fig 1 show the original segmented Image, Fig 2 shows the background subtraction of the image and fig 3 shows the foreground subtracted image using average median techniques.

This technique best suited for moving objects segmentation. The result shows the input image, the previous frame and after applying the Average Median and subtracting the background objects the foreground is alone displayed the result is displayed in the figures



FIG (1)

FIG (2)

FIG (3)

### C. Feature extraction using bounding box with color feature

Segmentation shows the objects and boundaries in an image. Each Pixel in the region has some similar characteristics like color, intensity, etc. In this work the feature extraction bounding box with color feature is adapted. For a specified image, an examination is performed where the intensity values of the image are additional than limit. In this Features is extracted by color and here the intensity value describes the color. The pixel values from the first hit of the intensity values from top, bottom, left and right are stored.



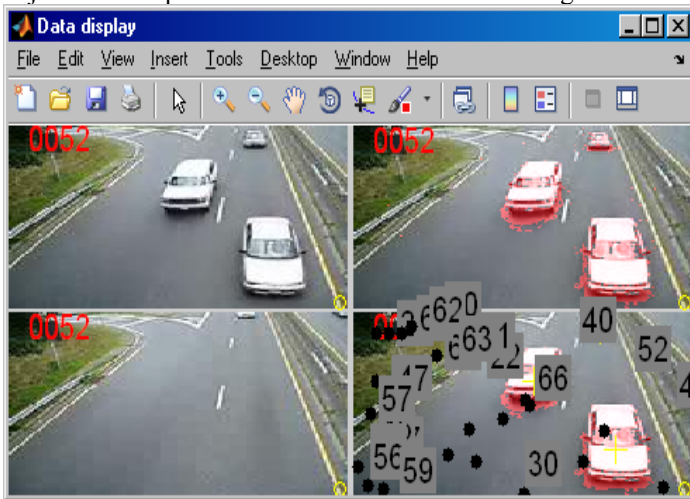
The figure below shows the output of the feature extraction using bounding box.



From the figure (a) shows the original video, (b) and (c) shows that the video of an moving object is detected using bounding box using color feature.

#### D. Object Identification and Object Tracking

Object tracking in video is performed by applying the Block Matching using three step approach of Intuitionistic Fuzzy to set the motion vector of the moving objects then finding the threshold of each object and detecting and tracking the objects which exceeds the threshold value as moving objects. The experimental results are shown in the figure.



Block matching of moving objects with co – ordinates

## VI. CONCLUSION

The proposed BMIFL algorithm reduces the computation time especially in the edge region of image. As the computation time is reduced, the total time to complete the detection of object is also reduced. This process has an advantage to control the quality of the image and the speed of the process as required, by controlling the allowable range. The distance is measured with the Intuitionistic fuzzy Divergence. The results obtained shows that the proposed BMIFL algorithm performs best in terms of execution time and speed. It also takes into account the uncertainty in the assignment of the membership degrees. The membership degree is set with the change in the hesitation degree and so the edge-detected results also vary with it. Thus with the change in hesitation degree, good edge-detected image is obtained.

## REFERENCES

- [1] Peter Mountney, Danail Stoyanov and Guang-Zhong Yang (2010). "Three-Dimensional Tissue Deformation Recovery and Tracking: Introducing techniques based on laparoscopic or endoscopic images." IEEE Signal Processing Magazine. 2010 July. Volume: 27". IEEE Signal Processing Magazine 27 (4): 14–24. doi:10.1109/MSP.2010.936728.
- [2] Lyudmila Mihaylova, Paul Bransett, Nishan Canagarajan and David Bull (2007). Object Tracking by Particle Filtering Techniques in Video Sequences; In: Advances and Challenges in Multisensor Data and Information. NATO Security Through Science Series, 8. Netherlands: IOS Press. pp. 260–268. ISBN 978-1-58603-727-7. CiteSeerX: 10.1.1.60.8510.
- [3] Kato, Hirokazu, and Mark Billinghurst (1999). "Marker Tracking and HMD Calibration for a Video-based Augmented Reality Conferencing System". IWAR '99 Proceedings of the 2nd IEEE and ACM International Workshop on Augmented Reality (IEEE Computer Society, Washington, DC, USA)
- [4] [http://en.wikipedia.org/wiki/Video\\_tracking](http://en.wikipedia.org/wiki/Video_tracking).
- [5] Shilpa Mehta (2008) Fuzzy control system for controlling traffic lights. Hong Kong IMECS. pp: 19-21.
- [6] Kok Khiang Tan, Marzuki Khalid and Rubiyah Yusof (1996) Intelligent traffic lights control by fuzzy logic. Malaysian J. Comput. Sci. pp: 29-35.
- [7] Barzegar, Davoudpour M, Meybodi MR, Sadeghian A and Tirandazian M (2011) Formalized learning automata with adaptive fuzzy Colored Petri net an application specific to managing traffic signals. Scientia Iranica. pp: 1-12.
- [8] Abdul Kareem, E.I. & Jantan, A. (2011). An Intelligent Traffic Light Monitor System using an Adaptive Associative Memory. International Journal of Information Processing and management. 2( 2): 23-39
- [9] Findler, N. V., Sudeep S., Ziya, M. & Serban, C. (1997). Distributed Intelligent Control of Street and Highway Ramp Traffic Signals. Engineering Applications of Artificial Intelligence 10(3):281- 292.
- [10] GiYoung, L., Kang J. and Hong Y. (2001). The optimization of traffic signal light using artificial intelligence. Proceedings of the 10th IEEE International Conference on Fuzzy Systems.
- [11] Wen, W. (2008). A dynamic and automatic traffic light control expert system for solving the road congestion problem. Expert Systems with Applications 34(4):2370-2381.
- [12] Tan, K., Khalid, M. and Yusof, R. (1996). Intelligent traffic lights control by fuzzy logic. Malaysian Journal of Computer Science, 9(2): 29-35
- [13] Fathy, M. and Siyal, M. Y. (1995). Real-time image processing approach to measure traffic queue parameters. Vision, Image and Signal Processing, IEEE Proceedings - 142(5):297-303.
- [14] Lei, J and Ozguner. U. (1999). Combined decentralized multi-destination dynamic routing and realtime traffic light control for congested traffic networks. In Proceedings of the 38th IEEE Conference on Decision and Control.
- [15] Huang, Q. and Miller, R. (2004). Reliable Wireless Traffic Signal Protocols for Smart
- [16] Intersections. Downloaded August 2011 from [http://www2.parc.com/spl/members/qluang/papers/tlights\\_itsa.pdf](http://www2.parc.com/spl/members/qluang/papers/tlights_itsa.pdf)
- [17] Di Febbraro, A., Giglio, D. and Sacco, N. (2004). Urban traffic control structure based on hybrid Petri nets. Intelligent Transportation Systems, IEEE Transactions on 5(4):224-237.
- [18] Nagel, K.A. and Schreckenberg, M.B. (1992). A cellular automation model for freeway Traffic. Downloaded September 2011 from [www.ptt.uniduisburg.de/fileadmin/docs/paper/1992/origca.pdf](http://www.ptt.uniduisburg.de/fileadmin/docs/paper/1992/origca.pdf).
- [19] Tavlakakis, A. K.(1999). Development of an Autonomous Adaptive Traffic Control System. European Symposium on Intelligent Techniques.
- [20] Chattaraj, A. Chakrabarti, S., Bansal, S., Halder, S. and . Chandra, A. (2008). Intelligent Traffic Control System using RFID. In Proceedings of the National Conference on Device, Intelligent System and Communication & Networking, India.
- [21] Osiwe Uchenna Chinyere, Oladipo Onaolapo Francisca, Onibere Emmanuel Amano," DESIGN AND SIMULATION OF AN INTELLIGENT TRAFFIC CONTROL SYSTEM", International Journal of Advances in Engineering & Technology, Vol. 1, Issue 5, pp. 47-57.

- [22] "Noise Reduction in Image Sequences using an Effective Fuzzy Algorithm", Mahmoud Saeidi, Khadijeh Saeidi, Mahmoud Khaleghi, World Academy of Science, Engineering and Technology 43 2008.
- [23] Linda G. Shapiro and George C. Stockman (2001): "Computer Vision", pp 279-325, New Jersey, Prentice-Hall, ISBN 0-13-030796-3.
- [24] "Image Feature Extraction Techniques and Their Applications for CBIR and Biometrics Systems", Ryszard S. Chora's, INTERNATIONAL JOURNAL OF BIOLOGY AND BIOMEDICAL ENGINEERING, Issue 1, Vol. 1, 2007, pp:6-16.
- [25] "A Moving Object Tracking and Velocity Determination", D.NEELIMA\*, KOPANATHI LAKSHMANA RAO\*, D.NEELIMA\* et al. / (IJAEST) INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES, ISSN: 2230-7818, Vol No. 11, Issue No. 1, 096 – 100, PP:96-100.
- [26] "Object Detection Using the Statistics of Parts", HENRY SCHNEIDERMAN AND TAKEO KANADE, International Journal of Computer Vision 56(3), 151–177, 2004.
- [27] [http://en.wikipedia.org/wiki/Block-matching\\_algorithm](http://en.wikipedia.org/wiki/Block-matching_algorithm).
- [28] Alper Yilmaz, Omar Javed, and Mubarak Shah Object Tracking: A survey. ACM Comput. Surv., 38(4):13, 2006.



## **A COMPARATIVE STUDY OF SOME BIOMETRIC SECURITY TECHNOLOGIES**

**BY**

**OGINI, NICHOLAS OLUWOLE**

**Department of Mathematics and Computer Science,**

**Delta State University, Abraka, Delta State.**

.

### **ABSTRACT**

Authentication plays a very critical role in security related applications. This is obvious from the breaches of information systems recorded around the world. This has become a major challenge to e-commerce and many other applications. One of the techniques that is implemented today to improve information security is biometrics, and this is gaining attention as the days go by. Having realized its value, biometrics is used in most systems today for the verification and identification of users as it overcomes the problems of being stolen, borrowed, forged or forgetting. In this paper therefore, we show the origin and types of biometrics, thier areas of application, and what to look out for in selecting a biometric technology.

### **INTRODUCTION**

Biometric technology is an automated method to allow the determination and verification of ones' identity based on one or more physical or behavioural characteristics. In simple terms, it turns one's personal features or attribute into a password to enable access into information systems. Uludag et al (2004).

The first use of biometrics technology was the finger printing in the 14th century by an European explorer Joao de Barros in China. It was followed sometimes in 1890 by Alphonse Bertilon who studied body mechanics and measurements this was to help in identification of criminals. This was used by the police until a failure caused it to be abandoned in the early 20th century, signature based biometric authentication procedures were developed, however the coming of the military and security agencies led to the development of this technology beyond the finger printing method. People can be

identified basically from attributes which can be expressed as physiological characteristics or behavioural characteristics. These technologies now serve as the backbone of highly secured systems for identification of individuals. Jain et al (2003).

The physiological biometrics consists of measurements and data gathered from the direct measurement of a part of the human body. Examples of physiological characteristics include hand geometry, facial recognition, finger print, iris scan, e.t.c. The indirect measurement of the unique characteristics of the human unique characteristics is the behavioural biometrics, examples are key strokes scan, signature scan, voice recognition e.t.c. However, the behavioural biometrics is impacted by time. Shoniregun (2003).

Uludag et al (2004) opines that for an ideal biometric, the system should possess the following

- Universality- each person should possess this characteristic
- Uniqueness- the biometric separates one individual from another (no two persons share that characteristic)
- Permanence- the biometric should resist ageing and other variations over time
- Collectability- it should be acquired easily for measurement
- Performance- the technology should provide accuracy, speed and robustness if used.
- Acceptability- the users of the biometric should have a degree of approval of a technology
- Circumvention- relates to the ease with which a trait might be imitated using an artifact or substitute

Some popular biometric techniques in use today include Finger print, Iris scan, Retina, Hand geometry, Face, Voice, and Signature.

## **METHODOLOGY**

The entire process of image processing starts from the receiving of visual information to the giving out of description of the scene from what is stored in the database, and this can be divided into five major stages, which are listed below.

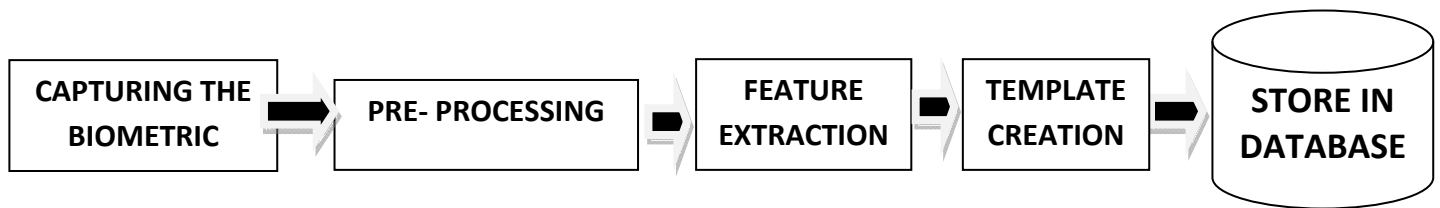


fig. 1: the entire enrollment process

- i. Enrollment: The first time an individual uses a biometric system is called enrollment. During the enrollment, biometric information from an individual is captured for storage. This is the interface between the real world and the system.
- ii. Pre processing: For efficiency of data, all the data acquired are pre processed to remove noise and enhance the features required for reference.
- iii. Feature extraction: This is extraction of the match points from the biometric that will be used for comparison.
- iv. Template creation: using an algorithm, the digital form of the biometric data is processed as match points for comparison with inputs for identification or verification.
- v. A database to store the information in the form of vector of numbers or an image with particular properties used to create a template that can be compared with the biometric data sent in as input when a user tries to gain access.

Thus a biometric system is essentially a pattern recognition system, which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. An important issue in designing a practical system is to determine how an individual is identified. Depending on the context, a biometric system can be either a verification system or an identification system.

## **SOME TYPES OF BIOMETRICS AND THEIR METHODOLOGIES**

### **FINGERPRINT SCAN**

The impression left by the patterns of the ridges of the finger pads of a human being are called fingerprints which can be obtained from the finger or the palm of the hand, the toe or the sole of the foot. It is the oldest of all the biometric techniques. the uniqueness of fingerprint also lies in the fact

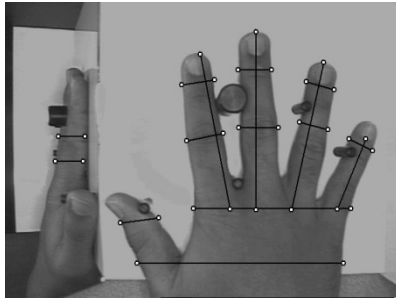
that even two fingers of the same individual can never produce an identical match in establishing the identity of an individual. Fingerprints serve an integral part of investigative measures as no two humans (including identical twins) can have exactly the same fingerprint.

There are a variety of approaches to fingerprint verification. The varieties of fingerprint devices available are more than any other biometric system at present. The traditional method uses the ink to get the finger print onto a piece of paper. This piece of paper is then scanned using a traditional scanner. Some of them try to emulate the police method of matching minutiae, others are straight pattern matching devices, and some adopt a unique approach all of their own. In modern approach, live fingerprint readers are used, they are based on optical, thermal, silicon or ultrasonic principles. It takes a digital scan of a person's fingertips and records its unique physical characteristics, such as whorls, arches, loops, ridges and furrow. They are based on reflection changes at the spots where finger papillary lines touch the reader surface. All the optical fingerprint readers comprise the source of light, the light sensor and a special reflection surface that changes the reflection according to the pressure. Some readers are fitted out with the processing and memory chips as well.



Fingerprint verification is a good choice for systems where adequate explanation and training can be provided to users and where the system is operated within a controlled environment. Many access applications seem to be based almost exclusively around fingerprints, due to the relatively low cost, small size and ease of integration. It is capable of good accuracy.

## **HAND GEOMETRY**



Source: [http://fingerchip.pagesperso-orange.fr/biometrics/types/hand/hand\\_features.jpg](http://fingerchip.pagesperso-orange.fr/biometrics/types/hand/hand_features.jpg)

Hand geometry is concerned with measuring the physical characteristics of the users hand and fingers, from a three-dimensional perspective. It measures and analyzes the overall structure, shape and proportions of the hand, e.g length, width and thickness of hand, fingers, hand curvature, knuckle shape, distance between joints and bone structure and translucency. It translates that information into a numerical template. This methodology may be suitable where we have larger user bases or users who may not access the system frequently and may therefore be less disciplined in their approach to the system. To use a hand scanner, you simply place your hand on a flat surface, aligning your fingers against several pegs to ensure an accurate reading. Then, a camera takes one or more pictures of your hand and the shadow it casts. Accuracy can be very high if desired.

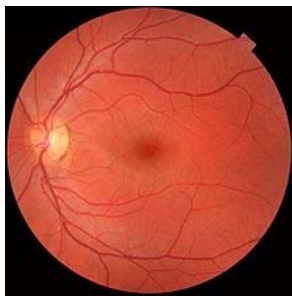
The hand and finger scanner/reader devices still maintain accuracy even when hands are dirty, which are good in construction areas; and also have the ability to work under extreme temperatures ranging from -30°F to +150°F. It is one of the more established methodologies; it offers a good balance of performance characteristics and is relatively easy to use.

Hand geometry readers are deployed in a wide range of scenarios, including time and attendance recording where they have proved extremely popular. Ease of integration into other systems and processes, coupled with ease of use makes hand geometry attractive to many biometric projects. Unlike fingerprints, human hand is not unique. However, hand geometry-based biometrics is not as intrusive as a fingerprint recognition system and hence may be sufficient enough to be used for verification (after the identity of the individual has been established through another mechanism).

## **VOICE VERIFICATION**

Speaker recognition systems discriminate between speakers by making use of the combination of physiological differences in the shape of vocal tracts and learned speaking habits. They are mostly passphrase-dependent. During the enrolment phase, a user is required to speak a particular passphrase (like a name, birth date, birth city, favourite colour, a sequence of numbers e.t.c) over a microphone for a certain number of times. This phrase is converted from analog to digital format, and the distinctive vocal characteristics such as pitch, cadence, and tone, are extracted and a speaker model is established. A template is then generated and stored for future comparisons. This is a potentially interesting; however, many of them have suffered in practice due to the variability of both transducers and local acoustics. In addition, the enrolment procedure has often been more complicated than with other biometrics leading to the perception of voice verification as unfriendly in some quarters.

### **RETINA SCANNING**



source:

[http://upload.wikimedia.org/wikipedia/commons/thumb/4/48/Fundus\\_photograph\\_of\\_normal\\_left\\_eye.jpg/220px-Fundus\\_photograph\\_of\\_normal\\_left\\_eye.jpg](http://upload.wikimedia.org/wikipedia/commons/thumb/4/48/Fundus_photograph_of_normal_left_eye.jpg/220px-Fundus_photograph_of_normal_left_eye.jpg)

This is an established technology where the unique patterns of the retina are scanned by a low intensity light source via an optical coupler. Retinal scanning has proved to be quite accurate in use but does require the user to look into a receptacle and focus on a given point. Retina scans are the most accurate. They capture the pattern of blood vessels in the eye. No two patterns are the same, even between the right and left eye, and identical twins. Nor do retinal patterns change with age. To get a usual sample, an individual must cooperate by keeping his head fixed and focusing on a target while an infrared beam is shown through the pupil. The reflected light is then measured and captured by a camera. This is not particularly convenient for those who avoid intimate contact with the source used for the scan and hence this has a few user-acceptance problems although the technology itself can work well. Retinas are also susceptible to diseases, such as glaucoma or cataracts which would defeat a system intended to

protect the elderly. It is believed to replace traditional ID methods such as P.I.N and virtually every other electronic device used for conducting business where identification is a requirement and prerequisite.

### **IRIS SCAN**



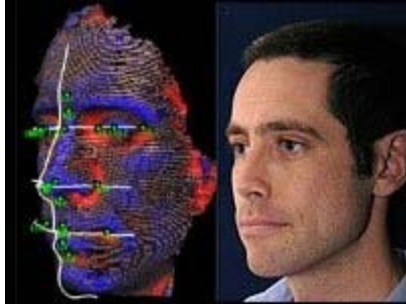
source: [http://3.bp.blogspot.com/-](http://3.bp.blogspot.com/-maCuJe2_2i8/TujHaEjAB1I/AAAAAAAAABeE/pG5zEtdeVQA/s320/connected-graphics_1080726a.jpg)

[maCuJe2\\_2i8/TujHaEjAB1I/AAAAAAAAABeE/pG5zEtdeVQA/s320/connected-graphics\\_1080726a.jpg](http://3.bp.blogspot.com/-maCuJe2_2i8/TujHaEjAB1I/AAAAAAAAABeE/pG5zEtdeVQA/s320/connected-graphics_1080726a.jpg)

The iris has coloured streaks and lines that radiate out from the pupil of the eye. A camera is used to take a picture of the iris. Iris scanning is the less intrusive of the eye related biometrics. It utilizes a conventional camera element and requires no intimate contact between user and reader. The person must be within 36 inches of the camera and focused on a target in order to get a quality scan. Cooperation of the individual is necessary, glasses and coloured contact lenses can change the template created from a single individual. The iris provides the most comprehensive biometric data after DNA. It has more unique information than any other single organ in the body. In this scanning, the characteristics of the iris are taken into account. About 266 unique points are recorded and converted into a 512 byte iris code (somewhat similar to barcode). The iris code constructed contains information the characteristics and position of the unique points. Since the scan is based on the size of the pupil, drugs dilating the eye could defeat an iris scan. Iris based biometric system are more secured than most other systems. However, ease of use and system integration has not traditionally been strong points with the iris scanning devices.

### **FACIAL SCAN**





source:<http://fingerchip.pagesperso-orange.fr/biometrics/types/face/laun.jpg>

The facial scan technique makes use of specific characteristics of the human face. It compares data from certain parts of the face with your face during a scan. Only certain parts of the face are used in this technique (the upper outlines of the eye sockets, the areas around the cheekbone, and the sides of the mouth) because these parts are hard to change with plastic surgery.

Face recognition systems can accurately verify the identity of a person standing two feet away under few seconds. A facial recognition system is used to authentically identify or verify a person from a digital image or a video frame from a video source. this is done by comparing selected facial features that are not easily altered (upper outlines of the eye sockets, the areas around the cheekbones, and the sides of the mouth) with those in the database.

## **SIGNATURE RECOGNITION SYSTEMS**



source: [http://www.epadlink.com/images/ePad-ink-w-hand\\_small.png](http://www.epadlink.com/images/ePad-ink-w-hand_small.png)

Signature recognition refers to authenticating the identity of a user by measuring handwriting signatures. In a signature recognition system, a person signs his or her name on a digitized graphic tablet or a PDA. This method enjoys a synergy with existing processes that other biometrics do not as people are used to signatures as a means of transaction related identity verification and mostly see nothing unusual in extending this to encompass biometrics. Signature verification devices have proved to be reasonably accurate in operation and obviously lend themselves to applications where the

signature is an accepted identifier. The signature is treated as a series of movements that contain unique biometric data, such as personal rhythm, acceleration, and stroke order, stroke count and pressure flow. The signature dynamics information is encrypted and compressed into a template. Signature recognition systems (for hand signatures) measure how a signature is signed and are different from electronic signatures, which treat a signature as a graphic image.

**TABLE 1 : RESULTS AND DISCUSSIONS**

	<b>Finger print</b>	<b>Iris scan</b>	<b>Retina</b>	<b>Hand geometry</b>	<b>Face</b>	<b>Voice</b>	<b>Signature</b>
<b>Universality</b>	High	High	High	High	High	High	High
<b>Uniqueness</b>	High	High	High	Average	Average	Average	High
<b>Permanence</b>	High	High	High	High	High	Average	High
<b>Performance</b>	High	High	High	Average	High	Average	Average
<b>Acceptability</b>	Average	Average	Average	High	High	High	High
<b>Circumvention</b>	Low	Low	Low	Average	Average	Average	Average
<b>Collectability</b>	High	Average	Average	High	High	Average	High
<b>Cost of device</b>	cheap	High	High	Low	Average	Average	High
<b>Device required</b>	Scanner	Camera	Camera	Scanner	Camera	Microphone telephone	Optic pan touch panel
<b>Social acceptability</b>	High	Average	Low	High	High	High	High
<b>Reliability</b>	Average	High	High	Average	average	average	Average

Biometric technologies have come to stay and play very vital roles in providing security through a good means of authentication. Most systems that have been able to withstand security challenges are biometric systems. However this is not without some issues such as , injuries or scars to fingers used for enrollment in fingerprint technology, eye diseases in retina and iris systems, cough in voice recognition e.t.c.

The reliability of a technology tends to be the inverse of the social acceptance of that technology. Fingerprints are socially accepted with some resistance from those that associate them with criminal

behaviour. Facial recognition is quite uncontroversial but equally has relatively high failure rates. It is generally regarded that eye scans are the most reliable form of biometrics. However, technology such as iris and retina scanning appears to have more social resistance due to its perceived intrusive nature, especially the retina. For this reason iris scanning is now more prevalent than the deeper retina scan.

Facial recognition is non intrusive, Cheap technology, but it is affected by changes in lighting, the person's hair, the age, and if the person wear glasses and it requires some camera equipment for user identification; thus, it is not likely to become popular until systems include cameras as standard equipment. For the Voice recognition, it is also non intrusive and has a high social acceptability it is a cheap technology but a person's voice can be easily recorded and used for unauthorised activities. The level of accuracy is also low as illness such as a cold can change a person's voice, making absolute identification difficult or impossible. Signature recognition non intrusive, it is a cheap technology, however, signature verification is designed to verify subjects based on the traits of their unique signature. As a result, individuals who do not sign their names in a consistent manner may have difficulty enrolling and verifying in signature verification. Retina scanning has a very high accuracy and there is no known way to replicate a retina and the eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to been taken with retinal scans to be sure the user is a living human being. It is however very intrusive and people have the stigma of thinking it is potentially harmful to the eye, also it is very expensive. Iris recognition is very high in accuracy. It shares similar attributes with the retina. However it requires a lot of memory for the data to be stored and it is very expensive. The fingerprint is also very high in accuracy. It is the most economical biometric authentication technique and one of the most developed biometrics and has become very easy to use. Its small storage space required for the biometric template reduces the size of the database memory required. Some people feel it is intrusive because it is related to criminal identification and it can make mistakes with the dryness or dirty of the finger's skin, as well as with the age (especially with children, because the size of their fingerprint changes quickly). Hand Geometry though it requires special hardware to use, it can be easily integrated into other devices or systems. It has no public attitude problems as it is associated most commonly with authorized access. The amount of data required to uniquely identify a user in a system is the smallest by far, allowing it to be used with SmartCards easily. It is however very expensive.

## CONCLUSION

Some. Some people consider the retina scan to be too intrusive and hence hesitant to expose themselves to scanning the least expensive and easiest to use is however the finger print technology. For highly sensitive systems, they may need to be updated regularly, and a multimodal (more than one) biometric technology will be a near perfect approach to providing security.

## REFERENCES

What is The Most Reliable Biometric Technology?

<http://www.chqconsulting.co.uk/reliable-biometric/>

What are the functions of biometric devices?

[http://www.ehow.com/facts\\_6087565\\_functions-biometric](http://www.ehow.com/facts_6087565_functions-biometric)

Advantages and disadvantages of technologies

<http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies>

Biometric Technology

[www.slideshare.net/biometric-technologythe-most-reliable-](http://www.slideshare.net/biometric-technologythe-most-reliable-)

How Reliable Is Biometric Technology?

[www.argus-global.co.uk/how-reliable-is-biometric-technology](http://www.argus-global.co.uk/how-reliable-is-biometric-technology)

Biometric Technologies: Security, Legal, and Policy Implications

<http://www.heritage.org/research/reports/2004/06/biometric-technologies-security-legal-and-policy-implications>

Uludag, U., Pankanti, S., Prabhakar, S, and A.K. Jain (2004), Biometric cryptosystems: issues and challenges, *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948-960.

An introduction to biometric recognition (2004) , Anil K. Jain , Arun Ross , Salil Prabhakar , IEEE ,

[www.csee.wvu.edu](http://www.csee.wvu.edu)

Shoniregun C.A. (2003), 'Are existing internet security measures guaranteed to protect user identity in the financial services industry?', *International Journal of Services, Technology and Management (IJSTM)*, vol. 4, no. 3, pp. 194–216; ISSN 1460-6720 (print), ISSN 1741-525X (online)

# Digital Images Encryption in Spatial Domain Based on Singular Value Decomposition and Cellular Automata

Ahmad Pahlavan Tafti

PhD Student, Department of Computer Science  
University of Wisconsin Milwaukee  
ahmad.pahlavantafti@ieee.org

Reyhaneh Maarefdoust

Sama technical and vocational training college, Islamic  
Azad University, Mashhad Branch,  
Mashhad, Iran.  
Maarefdost@yahoo.com

**Abstract**— Protection of digital images from unauthorized access is the main purpose of this paper. A reliable approach to encrypt a digital image in spatial domain is presented here. Our algorithm is based on the singular value decomposition and one dimensional cellular automata. First, we calculate the singular value decomposition (SVD) of the original image in which the features of the image are extracted and then pushed them into the one dimensional cellular automata to generate the robust secret key for the image authentication. SVD is used as a strong mathematical tool to decompose a digital image into three orthogonal matrices and create features that are rotation invariant.

We applied our proposed model on one hundred number of JPEG RGB images of size  $800 \times 800$ . The experimental results have illustrated the robustness, visual quality and reliability of our proposed algorithm.

**Keywords**- Digital Images Encryption; Spatial Domain Encryption; Cellular Automata, SVD.

## I. INTRODUCTION

Digital information like digital images and multimedia contents are widely used in many aspects such as meteorology, astronomy, radiology, robotics and surveillance systems. Validation and authentication of digital images are very important challenges for storing, retrieving and also transmitting of them.

Multimedia encryption has become the subject of very exhaustive research as its potential to transfer of information more securely. The encryption algorithms which have developed for text data are not suitable for multimedia data [1].

There are two main ways for digital images encryption. These are spatial domain and frequency domain encryption [2]. Spatial domain encryption is very simple where the frequency encryption is more complicated and reliable [2]. There are two level for digital images encryption; high-level and low-level. In the high-level encryption the content of the digital image is completely disordered and the original image is invisible. In

low-level encryption, the content of the digital image is understandable and visible [3].

In this paper we focused on the spatial domain and low-level encryption methods. Our proposed model is based on SVD (Singular Value Decomposition) and one dimensional cellular automata. We use the singular value decomposition to extract the features of the original image (Singular Values and Singular Vectors) to push them into the cellular automata to create a secret key. This key is so much related to the digital image that any small change in the content of digital image will definitely change the key value without any exception.

The rest of this paper is arranged as follows. In section 2 we describe one dimensional cellular automatas and their rules. Section 3 introduces the concepts of SVD and its uses. Section 4 describes the system design and section 5 focuses on experimental results. Conclusions presents in section 6.

## II. CELLULAR AUTOMATA

The history of cellular automata dates back to the 1940s with Stanislaw Marcin Ulam. This polish mathematician was interested in the evolution of graphic constructions generated by simple rules [4]. The base of his construction was a two-dimensional space divided into "cells", a sort of grid. Each of these cells could have two states: ON or OFF [5]. Cellular automata is a discrete dynamic model in space and time [5]. All of the cells arrange in the regular form and have a finite number of states. The states are updated with a local rule. Figure 1 shows a simple two state and one dimensional cellular automata with one line of cells. A specific cell can be either be on (value = 1= red) or off (value = 0= green). The closest cells to cell X are those to immediate left and right, moving along the lines connecting the nodes. The state of X at the time  $t + 1$  will be determined by the states of the cells within its neighborhood at the time t. [6].



Figure 1. One dimensional cellular automata with one neighborhood for cell X

We can set a local rule for each cellular automata. For example, we can estimate the value of cell X in time t+1 with the following rule [6]:

$$\text{Cell}[X]_{t+1} = \text{Cell}[X-1]_t (\text{OR}) \text{Cell}[X+1]_t$$

Assume that the input sequence is 01110 and we want to use the above rule for our cellular automata, then the output sequence will be 11111. Table 1 shows the output of this cellular automata.

TABLE 1. AN EXAMPLE OF CELLULAR AUTOMATA AND ITS RULE

Cell Number	0	1	2	3	4
Input Sequence (time t)	0	1	1	1	0
Cellular Automata Rule	$\text{Cell}[X]_{t+1} = \text{Cell}[X-1]_t (\text{OR}) \text{Cell}[X+1]_t$				
Output Sequence (time t+1)	1	1	1	1	1

We use one dimensional cellular automata with XOR local rule to create a secret key which we want to embed this key into the spatial domain of a digital image. The input sequence in our proposed model is the array list of the sum and mean of eigenvalues and eigenvectors.

### III. SINGULAR VALUE DECOMPOSITION

The basic theory of the SVD is reviewed in this section to show its power and ability to decompose any square or non-square digital image matrix into three orthogonal matrices that contain the useful features of the image. SVD can help us to select the dominant features in a digital image [7]. The SVD can decompose any real or complex  $n \times p$  matrix into product of three matrices, an orthogonal matrix U, a diagonal matrix S, and the transpose of an orthogonal matrix V as (1):

$$A_{n \times p} = U_{n \times n} S_{n \times p} V_{p \times p}^T \quad (1)$$

Where U and V are Orthogonal Matrices ;i.e.

$$U^T U = U U^T = I_{n \times n} \quad (2)$$

and

$$V^T V = V V^T = I_{p \times p} \quad (3)$$

Where the columns of U are called the Left Singular Vectors (Orthogonal Eigenvectors of  $AA^T$ ), S (the same dimensions as A) a diagonal matrix that has the Singular Values (the Square roots of the Eigen values of  $AA^T$  or  $A^T A$ ), and the columns of V called the Right Singular Vectors (Rows of  $V^T$ , Orthogonal Eigenvectors of  $ATA$ ). The SVD represents an expansion of the original data in a coordinate system where the covariance matrix is diagonal [8].

To calculate the SVD of the matrix A we can either apply the Golub-Reinsch Algorithm that use a finite sequences of the Householder Transformation or directly find the Eigen Values

and Eigen Vectors of  $AA^T$  and  $A^T A$ . The eigenvectors of  $A^T A$  make up the columns of V, the eigenvectors of  $AA^T$  make up the columns of U. where the singular values of S are the square roots of eigenvalues calculated from  $AA^T$  or  $A^T A$ . The singular values are the diagonal entries of the S matrix and are arranged in descending order. The singular values are always real numbers [9]. If the matrix A is a real matrix, then U and V are also real. Let us calculate the SVD of a  $3 \times 2$  matrix A using the Eigen analysis of  $A^T A$  and  $AA^T$ .

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} \quad (4)$$

First, we calculate  $B = A^T A$  and apply the Eigen Analysis formula to get the Eigenvalues and Eigenvectors of B as (9):

$$B X = \lambda X \quad (B - \lambda I) X = 0 \quad (5)$$

$$\text{We have } B = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \quad (6)$$

Thus, the Eigenvalues and normalized Eigenvectors are:

$$\lambda_1 = 3, V_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad (7)$$

$$\lambda_2 = 1, V_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \quad (8)$$

The Singular values can be calculated as:

$$\sigma_1 = \|AV_1\|_2 = \sqrt{\lambda_1} = \sqrt{3}; \quad (9)$$

$$\sigma_2 = \|AV_2\|_2 = \sqrt{\lambda_2} = 1 \quad (10)$$

Thus we can immediately calculate u1, u2.

$$u_1 = \frac{1}{\sigma_1} A V_1 = \frac{1}{\sqrt{6}} \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} \quad (11)$$

$$u_2 = \frac{1}{\sigma_2} A V_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} -1 \\ 1 \\ 0 \end{bmatrix} \quad (12)$$

u3 must be selected such that to be orthogonal to both u1, u2. Thus, it can be written as:

$$u_3 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} \quad (13)$$

Therefore, A can be decomposed as products of three matrices:

$$\begin{bmatrix} 1/\sqrt{6} & -1/\sqrt{2} & 1/\sqrt{3} \\ 1/\sqrt{6} & 1/\sqrt{2} & 1/\sqrt{3} \\ 2/\sqrt{6} & 0 & -1/\sqrt{3} \end{bmatrix} \begin{bmatrix} \sqrt{3} & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix} \quad (14)$$

### IV. PROPOSED MODEL

The main idea of our proposed algorithm is to create a robust secret key and embed it in the LSB of a specific layer of the original image, to encrypt it. Our proposed method is

based on spatial domain and low-level encryption approaches in which some data or secret key is embedded into the spatial domain of the original image for the authentication. We have implemented our algorithm on a set of one hundred images and calculated the Eigenvalues and Eigenvectors of  $B = A^T A$ . Then derived the Singular Values and Right and Left Singular Vectors of the original image based on the equations (7-13) and pushed the SVD features into one dimensional cellular automata to generate the secret key. First, we achieve the Singular Values and the Right and Left Singular Vectors of the Red matrix (Red layer of the RGB image) derived from input image and perform the same task for the Green matrix. Then we use one dimensional cellular automata with a particular rule to create the secret key based on those values. Next, we embed the bit sequence of the secret key into the LSB of the particular pixels of the Blue layer (Blue Matrix) in the original image.

Our proposed algorithm performs on a RGB JPEG image and generates a lossless PNG image with the RGB mode. We don't generate lossy compression format. Our algorithm may not only be used for RGB JPEG or PNG images, but also can be applied on the other types of digital images.

The embedding process is based on the cellular automata with XOR local rule (Table 2). Cellular automata have been implemented to create the required secret key bit sequence. We only use eight numbers of the original image's features to generate this key. These values consist of sum of eigenvalues, sum of eigenvectors, mean of eigenvalues and mean of eigenvectors of the image.

TABLE 2. OUR PROPOSED CELLULAR AUTOMATA WITH XOR LOCAL RULE

Cell Number	Input Value	Rule
0	Sum of all <i>Eigen values</i> Numbers of <i>Red Matrix</i> of the Original Image.	$Cell[X]_{t+1} = Cell[X-1]_t \text{ XOR } Cell[X+1]_t$
1	Mean of all <i>Eigenvalues</i> Numbers of <i>Red Matrix</i> of the Original Image.	
2	Sum of all <i>Eigenvectors</i> Numbers of <i>Red Matrix</i> of the Original Image.	
3	Mean of all <i>Eigenvectors</i> Numbers of <i>Red Matrix</i> of the Original Image.	
4	Sum of all <i>Eigenvalues</i> Numbers of <i>Green Matrix</i> of the Original Image.	
5	Mean of all <i>Eigenvalues</i> Numbers of <i>Green Matrix</i> of the Original Image.	
6	Sum of all <i>Eigenvectors</i> Numbers of <i>Green Matrix</i> of the Original Image.	
7	Mean of all <i>Eigenvectors</i> Numbers of <i>Green Matrix</i> of the Original Image.	

All of these values are easy to calculate and also exclusive for a particular matrix. Figure 2 shows the block diagram of the proposed method and Figure 3 illustrates the diagram of the proposed cellular automata to create a secret key base on these attributes of an image. We applied our proposed model on the input image of JPEG type, as shown in Figure 2, but

our model is suitable and applicable for any format of RGB digital image.

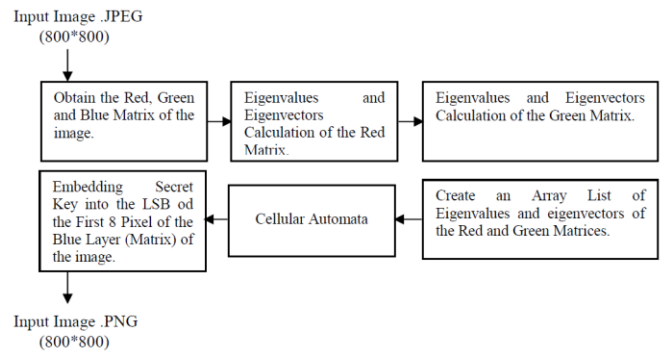


Figure 2. Block diagram of proposed model for digital images encryption in spatial domain.

The encryption algorithm in the frequency domain of the original image will be as follows:

#### Encryption Algorithm

**Input:** .JPEG RGB image to apply our proposed data embedding on it for image encryption.

**Output:** .PNG RGB image file.

**Step1:** Open the original image and obtain the Red, Green and Blue matrices of the image.

**Step2:** Calculate the Eigenvalues and Eigenvectors of the Red Matrix.

**Step3:** Calculate the Eigenvalues and Eigenvectors of the Green Matrix.

**Step4:** Perform the cellular automata rule according to the Table 2. This rule performs on the array list to create a Secret key.

**Step5:** Convert the Secret key to the binary representation.

**Step6:** Select the first eight pixels in the Blue Layer (Blue Matrix) and embed the binary sequences of Secret key into the LSB of each pixel for encryption.

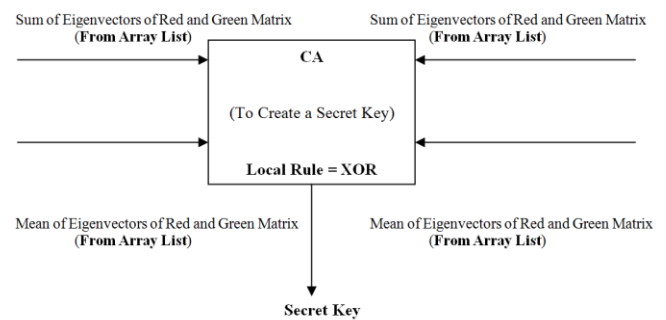


Figure 3. Block diagram of proposed cellular automata to create a secret key

The proposed algorithm has been implemented by C++ (C++ Builder XE2), which has the enough strength to work with digital images in any format.



## V. EXPERIMENTAL RESULTS

Four experimental results are given in this section to prove the performance and efficiency of the proposed model. These experimental results are as follows:

- Secret key sensitivity
- Diffusion
- Visual quality
- Time consumption

In order to evaluate the above aspects of our proposed method, we performed several tests on a sample dataset in our research laboratory. Our sample dataset contains 100 sets of RGB .JPEG images (size  $800 \times 800$ ). All of our codes are implemented with C++ (C++ Builder XE2).

### A. Secret key sensitivity

An ideal digital image encryption system should be sensitive with respect to the secret key. We mean a change of a single byte in the secret key should generate a completely different encrypted image and vice versa [10]. Table 3 shows the rate of secret key sensitivity.

TABLE 3. EVALUATION OF SECRET KEY SENSITIVITY AND ITS DEPENDENCY TO THE ORIGINAL IMAGE'S CHANGING

Image	Sum of Eigen Values (Red Layer)	Mean of Eigen Values (Red Layer)	
Sara	47	11	Original Image
	40	10	10 Pixels Changed
	38	9	20 Pixels Changed
Building	83	17	Original Image
	91	29	10 Pixels Changed
	87	21	20 Pixels Changed
Forest	69	19	Original Image
	82	13	10 Pixels Changed
	77	18	20 Pixels Changed

### B. Diffusion

In the second experiment the diffusion of our secret key is considered. Diffusion means that the output bits should depend on the input bits in a very complex way. In a secret key with good diffusion, if one bit of the plaintext is changed, then the secret key should change completely [11]. Figure 4 shows the diffusion chart of our proposed model of generating the secret key.

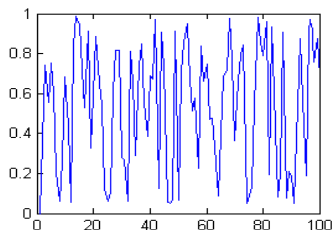


Figure 4. Diffusion Chart for Proposed Secret Key. Row indicates the number of images and column indicates the random number which is between 0 and 1.

### C. Visual quality

We have generated a .PNG image as the output of our method with lossless compression. The experiment also used a .PNG image of size  $800 \times 800$  as an input image. Figure 5 shows the original images and data embedded output PNG images which generated via our method to prove the visual quality of our method.

### D. Time consumption

We select the first eight pixels of the blue layer to embed our secret key into the original image, as we mentioned in section 4. Table 4 presents the results of different pixels selection with different time consumption. It shows that minimum time consumption is obtained by embedding the secret key into the first eight pixels of the original image.

TABLE 4. EVALUATION OF SECRET KEY SENSITIVITY AND ITS DEPENDENCY TO THE ORIGINAL IMAGE'S CHANGING

	First 8 Pixels	Middle 8 Pixels	Last 8 Pixels
Time consumption for embedding the secret key	0.27	0.76	0.92



Sara



Sara



Building



Building



Forest



Forest

Original Images

Encrypted Images

Figure 5. Encryption by the proposed algorithm and its visual quality

### E. Conclusion

In this paper, some dominant values possessed with singular value decomposition to design a potential method for digital image encryption. We present a low-level and spatial domain encryption method. In our proposed algorithm, a secret key was generated by eigenvalues and eigenvectors of the original image. One dimensional cellular automata with XOR local rule is employed to confuse the relationship between the original image and encrypted image. It means that the secret key is modified after obtaining those dominant values from the original image. The robustness of the proposed system is investigated in section 5, Table 3 and Figure 4 where we illustrated the secret key sensitivity and the diffusion of our proposed secret key. The experimental result demonstrated that our proposed algorithm has several invaluable features such as visual quality, good diffusion and enough sensitivity of secret key. We performed our proposed model on a sample dataset (.JPEG digital images (size  $800 \times 800$ )), but our algorithm could perform on various sizes and formats of digital images.

Although the algorithm presented in this paper has focused on digital image encryption, but it is not limited to this schemas and can be widely applied in the secure transmission of confidential digital signals over a network, Intranet or Internet.

### REFERENCES

- [1] Puech W, Rodrigues J. Crypto-Compression of medical images by selective encryption of DCT. *13<sup>th</sup> European Signal Processing Conference*. Turkey; 2005.
- [2] Ferguson N, Schneier B. *Practical cryptography*. John Wiley & Sons; 2010.
- [3] Van Droogenbroeck M, Benedett R. Techniques for a selective encryption of uncompressed and compressed images. *In proceeding of advanced concepts for intelligent vision systems*. Belgium; 2002.
- [4] Shatten A. *Cellular automata*. Institute of General Chemistry Vienna University of Technology. Austria; 1997.
- [5] Lafe O. Data compression and encryption using cellular automata transforms. *Artif, Intell*, Vol. 10, NO. 6, pp. 581-591; 1997.
- [6] Urias J. Cryptography primitive based on a cellular automata. *An Interdisciplinary Journal of Nonlinear Science*; 1998.
- [7] Mao K. Z. Identifying Critical Variables of Principal Components for Unsupervised Feature Selection. *IEEE Trans. Syst., Man, Cybern. B*, Vol. 35(2), pp. 339-344; 2005.
- [8] Alter O, Brown PO, Botstein D. Singular value decomposition for genome-wide expression data processing and modelling. *Proc Natl Acad Sci*, 97, 10101.USA; 2000.
- [9] Glob GH, Van Loan. *Matrix computation*. 2nd ed. Baltimore: Johns Hopkins University Press; 1989.
- [10] Ismail A, Amin M, Diab H. A digital image encryption algorithm based on a composition of two chaotic logistic maps. *International Journal of Network Security*, Vol. 11, No. 1, PP. 1-10; 2010.
- [11] Washington C. Introduction to cryptography with coding theory. Prentice Hall; 2006.

# Two-Level Approach for Web Information Retrieval

S. Subatra Devi  
Research Scholar  
PSVP Engineering College  
Chennai, Tamil Nadu, India.

Dr. P. Sheik Abdul Khader  
Professor & HOD  
BSA Crescent Engineering College  
Chennai, Tamil Nadu, India.

**Abstract** - One of the most challenging issues for web search engines is finding high quality web pages or pages with high popularity for users. The growth of the Web is increasing day to day and retrieving the information, which is satisfied for the user has become a difficult task. The main goal of this paper is to retrieve more number of, most relevant pages. For which, an approach with two-levels are undergone. In the first level, the topic keywords are verified with the title of the document, the snippet, and the URL path. In the second level, the page content is verified. This algorithm produces efficient result which is being proved experimentally on different levels.

**Keywords**- Information Retrieval; Crawler; Snippet.

## I. INTRODUCTION

Crawling has been the subject of widespread research and presently web crawling has been studied in diverse aspects. The web crawler is a program that searches the information related to the user's topic [13] and provides the reliable result. It is not necessary for the crawler to collect all web pages. The crawler selects only required pages [10] and retrieves relevant pages which are satisfied to the user.

In this paper, the topic keywords are given to three search engines namely, Google, Yahoo and MSN. The top 10 URL's that exists in common to all the three search engines are considered as the seed URL's during the initial iteration. Here, the crawler has three possibilities in the first level. For the given top 10 URL's, the three possibilities namely, the title of the document, the snippet and the URL path are verified with the given topic. If the topic keywords exist in any two or in all the three possibilities, then the pages are considered as relevant pages for the next iteration. If the keywords exist only in one of the three possibilities, then it is considered as an irrelevant page and not included for the next iteration. This makes the algorithm to consider the most relevant pages during the initial stage of the crawling.

In the second level of crawling, the topic keywords are verified with the page content. If the content of the page have more number of topic keywords, then it is considered as a relevant page and the crawler moves to the next stage of crawling. With each and every stage of crawling, the irrelevant pages are filtered out in the first level. This makes the crawling efficient and retrieves the most relevant pages effectively.

This paper is structured as follows. Section 2 shows the related work. In Section 3, the novel algorithm for web crawling process is proposed. Section 4 shows the experimental results and the performance evaluation of the proposed work. Finally, Section 5 concludes the paper.

## II. RELATED WORK

"Fish Search" is one of the first dynamic search heuristics, that capitalizes on the intuition in which relevant documents often have relevant neighbors. This algorithm [1] searches the query dynamically by the value 0 and 1 and finds the information in the distributed hypertext. The search results are ranked based on user preferences in content and link and integrated to rank the results [4]. TF-IDF method is the base method for retrieving the keywords from the page content. In addition to that, Vector similarity method [2] is applied.

The topic keyword is used as a base in several algorithms. Topic distillation is performed in [3]. A Focused crawling [12], analyze its crawl boundary that are likely to be most relevant for the crawler [10]. Text search based on the keyword [8] is the basic concept for the information retrieval algorithms. The hyperlink, linking from the parent to the child URL is based on several methods. Link score is calculated based on the division score in algorithm [11]. Based on multi-information, the relevant pages are retrieved in [9]. There are several algorithms based on content and link strategy. The algorithm based on hyperlink and content relevance

and on HITS is presented as Heuristic search [5]. Comparative study of two ranking algorithms namely page rank and users rank are studied [13]. Multiple information's are used to improve the Shark-search algorithm [7]. Breadth-first method is used to produce high relevant pages [6] which is applied in the proposed method.

### III. PROPOSED ALGORITHM

In the proposed method, the topic is given to the search engines and the top 10 URL's are considered as the input to the proposed method. For these URL's, the initial preference is given for the title of the document, the snippet and the parent URL's, which are considered at Level1. If any two of these or all the three possibilities contains the keyword, then these URL's are considered as relevant URL's and are given to Level2. In Level2, the page content of the document is verified with the frequency of the keyword.

#### A. Seed URL Extraction

Initially, the topic keywords are given to the three different search engines Google, Yahoo and MSN. The top ten URL's that exists commonly in all the three search engines are taken, and considered for evaluation. These URL's are considered as the seed URL's.

#### B. Relevancy Prediction

The relevancy of the document is predicted based on the title of the document, the snippet and the parent URL, at level1 and the page content method at level2. These possibilities are discussed below. This approach specifies the relevancy more precisely.

##### 1) The Title of the Document

The title of the document is verified whether it contains the topic keyword. The document title consists of a set of words. Each and every word  $w_i$  is compared with the given keyword  $KW_i$ .

$$T_i = \{w_1, w_2, w_3, \dots, w_n\}$$

Here,  $T_i$  represents the title of the document which consists of a set of words  $w_i$ . The relevancy of the title of the document is computed as

$$RS_{TOD} = \frac{KW_T}{W_T}$$

Where  $KW_T$  represents the number of keywords in the title and  $W_T$  represents the total number of words present in the title of the document.

The relevancy of the title of the document is evaluated based on the number of keywords existing in the title with the total number of words in the title.

##### 2) The Snippet

Here, the Snippet is checked if it contains the topic keywords. The snippet gives the brief information of what the document page consists of. The relevancy is determined as follows

$$RS_{SNIP} = \frac{KW_{SNIP}}{W_{SNIP}}$$

$KW_{SNIP}$  represents the total number of keywords present in the Snippet and  $W_{SNIP}$  represents the total number of words in the Snippet. The relevancy is more if all the keywords are present in the snippet.

##### 3) The Parent URL

The top 10 URL's generated from the search engine are considered as the parent URL's. These URL's are checked if it contains the anchor text. The number of keywords appearing in the parent URL is checked. For this, the division method is used. If all the keywords are present in the parent URL, then its relevancy is 1, otherwise the relevancy depends on the percentage value of the anchor text appearing on the parent link.

During the initial iteration, the URL will be acting as the parent URL. For the forthcoming iterations, the outgoing link of the parent URL will be the child URL, i.e., the link URL.

The relevancy of the parent URL is calculated as follows

$$RS_{PU} = \frac{KW_{PU}}{W_{PU}}$$

Where  $KW_{PU}$  represents the number of keywords in the parent URL and  $W_{PU}$  represents the total number of words in the parent URL.

##### 4) The Page Content

The text content or the page content of the document is given the next preference which is considered at level2. The keywords are extracted

from the page content using stop word removal, stemming method and finally the tokens are extracted. The frequencies of the tokens are found and the tokens are arranged in an order such that the token with higher frequency occurs first. The given topic keywords are compared with these set of tokens arranged based on the frequency.

If the frequency of the keyword is more, then that particular document is considered to be a more relevant document. If the frequency of the keyword is in an average, then it is considered as a relevant document. Otherwise, it is considered as an irrelevant document.

The relevancy score of the page content of the document is computed as follows

$$RS_{PC} = \frac{KW_{PC}}{W_{PC}}$$

Here,  $KW_{PC}$  represents the frequency of the topic keyword present in the page content and  $W_{PC}$  represents the total number of tokens present in the content of the document.

#### 5) The Relevancy Score

The relevancy score of the document for each URL is computed based on the method specified above. The aggregate of the relevancies specified above are formed by summing the weighted individual relevancy score.

$$\text{Relevancy-Score} = \alpha_1(RS_{TOD} * wt_1 + RS_{SNIP} * wt_2 + RS_{PU} * wt_3) + \alpha_2(RS_{PC} * wt_4)$$

Here  $wt_1$ ,  $wt_2$ ,  $wt_3$  and  $wt_4$  are the weights which are used to normalize the relevancy scores. The values of these weights vary between 0 and 1, inclusively. Based on these weights, the value of the weights can be increased to increase the importance of the particular relevancy.

After finding the relevancy score, it is compared with the specified threshold value. If the relevancy score is more than the threshold value, then the document is considered as the more relevant document. These documents URL are placed in the URL queue. The outgoing links of the parent URL are fetched based on the relevancy and placed in the URL queue. The same process described in the earlier steps is performed sequentially for all the pages in the URL queue until the URL gets empty.

## IV. EXPERIMENTAL RESULTS

The top 10 URL's which has been selected from the search engines are given as input to the proposed algorithm. The level1 process, which are the title, snippet and the parent URL are checked if it contains the topic keyword. The topic given for evaluation is 'query processing and optimization'.

For this topic, three of the URL's contains all the three possibilities of level1, four URL's contains the title, snippet and three URL's consists the topic keyword in title alone. The topic keywords present in all the three possibilities namely, the title, snippet and the parent URL are considered to be more relevant. The topic keywords occurring in any two are considered as relevant and in any one possibility is considered as least relevant and it is not considered for level2.

After the completion of level1, then the level2 is considered, which is the combination of level1 and the page content relevancy. The relevant pages at level1 are considered for level2, and the irrelevant pages are not considered during the initial iteration for level2. This removes the unwanted pages in the initial stage of crawling and skews the search to more relevant pages. The relevancy score for the different URL's are listed in Table1.

TABLE I. RELEVANCY SCORE AT LEVEL1 AND LEVEL2

S.No.	Parent URL	Relevancy score at Level1	Relevancy score at Level2
1	cs.iusb.edu/technical_reports/TR-20080105-1.pdf	2.27	3.0
2	www.spatial.cs.umn.edu/Book/slides/ch5revised.ppt	1.60	2.85
3	www.slideshare.net/signer/query-processing-and-optimisation	2.35	3.15
4	my.safaribooksonline.com/.../query-processing-and-optimization/ch0...	2.56	3.35
5	sce.umkc.edu/~kumarv/cs470/query-processing.pdf	2.47	3.20
6	webdocs.cs.ualberta.ca/~zaiane/courses/cmput391-02/.../sld004.htm	1.30	-
7	www.youtube.com/watch?v=GYQZpYEaNVk	1.25	-
8	www.youtube.com/watch?v=bI_UOHLuz7w	1.21	-

9	homepages.inf.ed.ac.uk/li	1.42	2.56
10	bkin/teach/dbs12/set5.pdf cnx.org > Content	1.35	2.45

This relevancy score is calculated for the parent URL, which is the seed URL during the initial iteration. The same process is repeated for each outgoing link and the relevancy is checked. The URL's having the least relevancy score at Level2 is discarded, and the URL's having the more relevancies is taken for consideration during the next iteration.

The total numbers of relevant pages retrieved at various levels are indicated in Figure1. The graph compares the total number of pages crawled with the number of relevant pages retrieved.

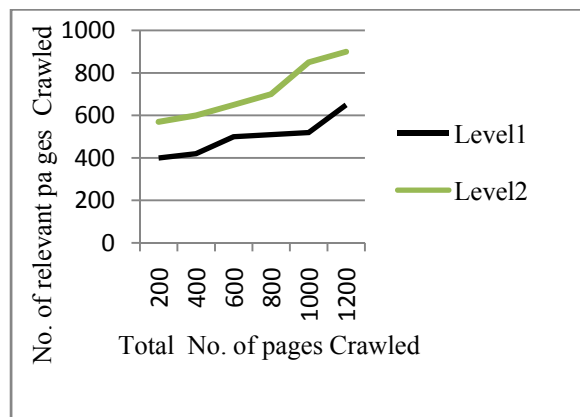


Figure1: Relevant pages crawled during Level 1 and Level 2

The graph indicates that the more number of relevant pages are retrieved at level1, since the irrelevant pages are discarded in the initial crawling. After level2, the most relevant pages are retrieved for the given topic.

For evaluating the efficiency, the experimentation is performed on different topics and the relevancy is checked. Different values for the weights are given to check the efficiency. It clearly indicates that the proposed algorithm retrieves the most relevant pages effectively.

## V. CONCLUSION & FUTURE WORK

In this paper, the two levels are considered for an efficient result. At level1, the title, the snippet and the parent URL are verified for relevancy. Based on level1 relevancy, the URL's are moved to level2.

This retrieves the more number of most relevant pages at the beginning of the crawling. It has been proved experimentally that the proposed algorithm retrieves the most relevant pages efficiently from the initial stage of crawling.

The major issue on future work is to do test with large volume of web pages. The future work also includes optimizing the code and the URL queue, which makes the crawler to retrieve maximum number of relevant pages in faster way.

## REFERENCES

- [1] P. De Bra, G-J Houben, Y. Kornatzky, and R. Post, "Information Retrieval in Distributed Hypertexts", in the Proceedings of RIAO'94, Intelligent Multimedia, Information Retrieval Systems and Management, New York, NY, 1994.
- [2] Yang Yongsheng, Wang Hui, "Implementation of Focused crawler", Journal of computers Vol. 6, No: 1, January 2011.
- [3] K.Bharat and M.Henzinger, "Improved Algorithms for Topic Distillation in a Hyperlinked Environment", In proc. Of the ACM SIGIR '98 conference on Research and Development in Information Retrieval.
- [4] J.Jayanthi, Dr. K.S. Jayakumar, "An Integrated Page Ranking Algorithm for Personalized Web Search", International Journal of Computer Applications, 2011.
- [5] Lili Yan, Wencai Du, Yingbin wei and Henian chen, "A novel heuristic search algorithm based on hyperlink and relevance strategy for Web Search", 2012, Advances in Intelligent and Soft Computing.
- [6] M. Najork and J.L. Wiener. "Breadth-first Crawling yields high-quality pages", In Proceedings of the Tenth Conference on World Wide Web, Hong Kong, Elsevier Science, May 2001, pp. 114–118.
- [7] Zhumin Chen; Jun Ma; Jingsheng Lei; Bo Yuan; Li Lian, "An Improved Shark-Search Algorithm Based on Multi-information", Fourth International Conference on Fuzzy Systems and Knowledge Discovery, pp: 659 – 658, Aug 24-27, 2007.

- [8] Lixin Hanna, Guihai Chen, "The HWS hybrid web search, Information and Software Technology", Vol: 48, No: 8, Pp: 687-695, 2006.
- [9] Shalin shah, "Implementing an Effective Web Crawler", September 2006.
- [10] S. Chakrabarti, M. van den Berg, and B. Dom, "Focused Crawling: A New Approach for Topic-Specific Resource Discovery", In Proc. 8th WWW, 1999.
- [11] Debashis Hati and Amritesh Kumar, "An Approach for Identifying URLs Based on Division Score and Link Score in Focused Crawler", International Journal of Computer Applications, Vol. 2, no. 3, May 2010.
- [12] Ahmed Patel and Nikita Schmidt, "Application of structured document parsing to focused web crawling", Computer Standards & Interfaces, Vol. 33, no. 3, pp. 325-331, March 2011.
- [13] Akshata D.Deore, Prof. R.L. Paikrao, "Ranking based web search algorithms", International Journal of Scientific and Research Publications, Oct 2012.



## IJCSIS REVIEWERS' LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA  
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia  
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA  
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway  
Assoc. Prof. N. Jaisankar, VIT University, Vellore, Tamilnadu, India  
Dr. Amogh Kavimandan, The Mathworks Inc., USA  
Dr. Ramasamy Mariappan, Vinayaka Missions University, India  
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China  
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA  
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico  
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India  
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania  
Dr. Junjie Peng, Shanghai University, P. R. China  
Dr. Ilhem LENGILIZ, HANA Group - CRISTAL Laboratory, Tunisia  
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India  
Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain  
Prof. Dr.C.Suresh Gnana Dhas, Anna University, India  
Mrs Li Fang, Nanyang Technological University, Singapore  
Prof. Pijush Biswas, RCC Institute of Information Technology, India  
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia  
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India  
Mr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand  
Mr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G.)/ Dimat Raipur, India  
Mr. Hayder N. Jasem, University Putra Malaysia, Malaysia  
Mr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India  
Mr. R. S. Karthik, C. M. S. College of Science and Commerce, India  
Mr. P. Vasant, University Technology Petronas, Malaysia  
Mr. Wong Kok Seng, Soongsil University, Seoul, South Korea  
Mr. Praveen Ranjan Srivastava, BITS PILANI, India  
Mr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong  
Mr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia  
Dr. Rami J. Matarneh, Al-isra Private University, Amman, Jordan  
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria  
Dr. Riktesh Srivastava, Skyline University, UAE  
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia  
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt  
and Department of Computer science, Taif University, Saudi Arabia  
Mr. Tirthankar Gayen, IIT Kharagpur, India  
Ms. Huei-Ru Tseng, National Chiao Tung University, Taiwan

Prof. Ning Xu, Wuhan University of Technology, China  
Mr Mohammed Salem Binwahlan, Hadhramout University of Science and Technology, Yemen  
& Universiti Teknologi Malaysia, Malaysia.  
Dr. Aruna Ranganath, Bhoj Reddy Engineering College for Women, India  
Mr. Hafeezullah Amin, Institute of Information Technology, KUST, Kohat, Pakistan  
Prof. Syed S. Rizvi, University of Bridgeport, USA  
Mr. Shahbaz Pervez Chattha, University of Engineering and Technology Taxila, Pakistan  
Dr. Shishir Kumar, Jaypee University of Information Technology, Wakanaghat (HP), India  
Mr. Shahid Mumtaz, Portugal Telecommunication, Instituto de Telecomunicações (IT) , Aveiro, Portugal  
Mr. Rajesh K Shukla, Corporate Institute of Science & Technology Bhopal M P  
Dr. Poonam Garg, Institute of Management Technology, India  
Mr. S. Mehta, Inha University, Korea  
Mr. Dilip Kumar S.M, University Visvesvaraya College of Engineering (UVCE), Bangalore University, Bangalore  
Prof. Malik Sikander Hayat Khiyal, Fatima Jinnah Women University, Rawalpindi, Pakistan  
Dr. Virendra Gomase , Department of Bioinformatics, Padmashree Dr. D.Y. Patil University  
Dr. Irraivan Elamvazuthi, University Technology PETRONAS, Malaysia  
Mr. Saqib Saeed, University of Siegen, Germany  
Mr. Pavan Kumar Gorakavi, IPMA-USA [YC]  
Dr. Ahmed Nabih Zaki Rashed, Menoufia University, Egypt  
Prof. Shishir K. Shandilya, Rukmani Devi Institute of Science & Technology, India  
Mrs.J.Komala Lakshmi, SNR Sons College, Computer Science, India  
Mr. Muhammad Sohail, KUST, Pakistan  
Dr. Manjaiah D.H, Mangalore University, India  
Dr. S Santhosh Baboo, D.G.Vaishnav College, Chennai, India  
Prof. Dr. Mokhtar Beldjehem, Sainte-Anne University, Halifax, NS, Canada  
Dr. Deepak Laxmi Narasimha, Faculty of Computer Science and Information Technology, University of Malaya, Malaysia  
Prof. Dr. Arunkumar Thangavelu, Vellore Institute Of Technology, India  
Mr. M. Azath, Anna University, India  
Mr. Md. Rabiul Islam, Rajshahi University of Engineering & Technology (RUET), Bangladesh  
Mr. Aos Alaa Zaidan Ansaef, Multimedia University, Malaysia  
Dr Suresh Jain, Professor (on leave), Institute of Engineering & Technology, Devi Ahilya University, Indore (MP) India,  
Dr. Mohammed M. Kadhum, Universiti Utara Malaysia  
Mr. Hanumanthappa. J. University of Mysore, India  
Mr. Syed Ishtiaque Ahmed, Bangladesh University of Engineering and Technology (BUET)  
Mr Akinola Solomon Olalekan, University of Ibadan, Ibadan, Nigeria  
Mr. Santosh K. Pandey, Department of Information Technology, The Institute of Chartered Accountants of India  
Dr. P. Vasant, Power Control Optimization, Malaysia  
Dr. Petr Ivankov, Automatika - S, Russian Federation

Dr. Utkarsh Seetha, Data Infosys Limited, India  
Mrs. Priti Maheshwary, Maulana Azad National Institute of Technology, Bhopal  
Dr. (Mrs) Padmavathi Ganapathi, Avinashilingam University for Women, Coimbatore  
Assist. Prof. A. Neela madheswari, Anna university, India  
Prof. Ganesan Ramachandra Rao, PSG College of Arts and Science, India  
Mr. Kamanashis Biswas, Daffodil International University, Bangladesh  
Dr. Atul Gonsai, Saurashtra University, Gujarat, India  
Mr. Angkoon Phinyomark, Prince of Songkla University, Thailand  
Mrs. G. Nalini Priya, Anna University, Chennai  
Dr. P. Subashini, Avinashilingam University for Women, India  
Assoc. Prof. Vijay Kumar Chakka, Dhirubhai Ambani IICT, Gandhinagar ,Gujarat  
Mr Jitendra Agrawal, : Rajiv Gandhi Proudhyogiki Vishwavidyalaya, Bhopal  
Mr. Vishal Goyal, Department of Computer Science, Punjabi University, India  
Dr. R. Baskaran, Department of Computer Science and Engineering, Anna University, Chennai  
Assist. Prof, Kanwalvir Singh Dhindsa, B.B.S.B.Engg.College, Fatehgarh Sahib (Punjab), India  
Dr. Jamal Ahmad Dargham, School of Engineering and Information Technology, Universiti Malaysia Sabah  
Mr. Nitin Bhatia, DAV College, India  
Dr. Dhavachelvan Ponnurangam, Pondicherry Central University, India  
Dr. Mohd Faizal Abdollah, University of Technical Malaysia, Malaysia  
Assist. Prof. Sonal Chawla, Panjab University, India  
Dr. Abdul Wahid, AKG Engg. College, Ghaziabad, India  
Mr. Arash Habibi Lashkari, University of Malaya (UM), Malaysia  
Mr. Md. Rajibul Islam, Ibnu Sina Institute, University Technology Malaysia  
Professor Dr. Sabu M. Thampi, .B.S Institute of Technology for Women, Kerala University, India  
Mr. Noor Muhammed Nayeem, Université Lumière Lyon 2, 69007 Lyon, France  
Dr. Himanshu Aggarwal, Department of Computer Engineering, Punjabi University, India  
Prof R. Naidoo, Dept of Mathematics/Center for Advanced Computer Modelling, Durban University of Technology, Durban,South Africa  
Prof. Mydhili K Nair, M S Ramaiah Institute of Technology(M.S.R.I.T), Affiliated to Visweswaraiah Technological University, Bangalore, India  
M. Prabu, Adhiyamaan College of Engineering/Anna University, India  
Mr. Swakkhar Shatabda, Department of Computer Science and Engineering, United International University, Bangladesh  
Dr. Abdur Rashid Khan, ICIT, Gomal University, Dera Ismail Khan, Pakistan  
Mr. H. Abdul Shabeer, I-Nautix Technologies,Chennai, India  
Dr. M. Aramudhan, Perunthalaivar Kamarajar Institute of Engineering and Technology, India  
Dr. M. P. Thapliyal, Department of Computer Science, HNB Garhwal University (Central University), India  
Dr. Shahaboddin Shamshirband, Islamic Azad University, Iran  
Mr. Zeashan Hameed Khan, : Université de Grenoble, France  
Prof. Anil K Ahlawat, Ajay Kumar Garg Engineering College, Ghaziabad, UP Technical University, Lucknow  
Mr. Longe Olumide Babatope, University Of Ibadan, Nigeria  
Associate Prof. Raman Maini, University College of Engineering, Punjabi University, India

Dr. Maslin Masrom, University Technology Malaysia, Malaysia  
Sudipta Chattopadhyay, Jadavpur University, Kolkata, India  
Dr. Dang Tuan NGUYEN, University of Information Technology, Vietnam National University - Ho Chi Minh City  
Dr. Mary Lourde R., BITS-PILANI Dubai , UAE  
Dr. Abdul Aziz, University of Central Punjab, Pakistan  
Mr. Karan Singh, Gautam Budtha University, India  
Mr. Avinash Pokhriyal, Uttar Pradesh Technical University, Lucknow, India  
Associate Prof Dr Zuraini Ismail, University Technology Malaysia, Malaysia  
Assistant Prof. Yasser M. Alginahi, College of Computer Science and Engineering, Taibah University, Madinah Munawwarah, KSA  
Mr. Dakshina Ranjan Kisku, West Bengal University of Technology, India  
Mr. Raman Kumar, Dr B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India  
Associate Prof. Samir B. Patel, Institute of Technology, Nirma University, India  
Dr. M.Munir Ahamed Rabbani, B. S. Abdur Rahman University, India  
Asst. Prof. Koushik Majumder, West Bengal University of Technology, India  
Dr. Alex Pappachen James, Queensland Micro-nanotechnology center, Griffith University, Australia  
Assistant Prof. S. Hariharan, B.S. Abdur Rahman University, India  
Asst Prof. Jasmine. K. S, R.V.College of Engineering, India  
Mr Naushad Ali Mamode Khan, Ministry of Education and Human Resources, Mauritius  
Prof. Mahesh Goyani, G H Patel Collge of Engg. & Tech, V.V.N, Anand, Gujarat, India  
Dr. Mana Mohammed, University of Tlemcen, Algeria  
Prof. Jatinder Singh, Universal Institutiion of Engg. & Tech. CHD, India  
Mrs. M. Anandhavalli Gauthaman, Sikkim Manipal Institute of Technology, Majitar, East Sikkim  
Dr. Bin Guo, Institute Telecom SudParis, France  
Mrs. Maleika Mehr Nigar Mohamed Heenaye-Mamode Khan, University of Mauritius  
Prof. Pijush Biswas, RCC Institute of Information Technology, India  
Mr. V. Bala Dhandayuthapani, Mekelle University, Ethiopia  
Dr. Irfan Syamsuddin, State Polytechnic of Ujung Pandang, Indonesia  
Mr. Kavi Kumar Khedo, University of Mauritius, Mauritius  
Mr. Ravi Chandiran, Zagro Singapore Pte Ltd. Singapore  
Mr. Milindkumar V. Sarode, Jawaharlal Darda Institute of Engineering and Technology, India  
Dr. Shamimul Qamar, KSJ Institute of Engineering & Technology, India  
Dr. C. Arun, Anna University, India  
Assist. Prof. M.N.Birje, Basaveshwar Engineering College, India  
Prof. Hamid Reza Naji, Department of Computer Enigneering, Shahid Beheshti University, Tehran, Iran  
Assist. Prof. Debasis Giri, Department of Computer Science and Engineering, Haldia Institute of Technology  
Subhabrata Barman, Haldia Institute of Technology, West Bengal  
Mr. M. I. Lali, COMSATS Institute of Information Technology, Islamabad, Pakistan  
Dr. Feroz Khan, Central Institute of Medicinal and Aromatic Plants, Lucknow, India  
Mr. R. Nagendran, Institute of Technology, Coimbatore, Tamilnadu, India  
Mr. Amnach Khawne, King Mongkut's Institute of Technology Ladkrabang, Ladkrabang, Bangkok, Thailand

Dr. P. Chakrabarti, Sir Padampat Singhanian University, Udaipur, India  
Mr. Nafiz Imtiaz Bin Hamid, Islamic University of Technology (IUT), Bangladesh.  
Shahab-A. Shamshirband, Islamic Azad University, Chalous, Iran  
Prof. B. Priestly Shan, Anna Univeristy, Tamilnadu, India  
Venkatramreddy Velma, Dept. of Bioinformatics, University of Mississippi Medical Center, Jackson MS USA  
Akshi Kumar, Dept. of Computer Engineering, Delhi Technological University, India  
Dr. Umesh Kumar Singh, Vikram University, Ujjain, India  
Mr. Serguei A. Mokhov, Concordia University, Canada  
Mr. Lai Khin Wee, Universiti Teknologi Malaysia, Malaysia  
Dr. Awadhesh Kumar Sharma, Madan Mohan Malviya Engineering College, India  
Mr. Syed R. Rizvi, Analytical Services & Materials, Inc., USA  
Dr. S. Karthik, SNS College of Technology, India  
Mr. Syed Qasim Bukhari, CIMET (Universidad de Granada), Spain  
Mr. A.D.Potgantwar, Pune University, India  
Dr. Himanshu Aggarwal, Punjabi University, India  
Mr. Rajesh Ramachandran, Naipunya Institute of Management and Information Technology, India  
Dr. K.L. Shunmuganathan, R.M.K Engg College, Kavaraipeitai, Chennai  
Dr. Prasant Kumar Pattnaik, KIST, India.  
Dr. Ch. Aswani Kumar, VIT University, India  
Mr. Ijaz Ali Shoukat, King Saud University, Riyadh KSA  
Mr. Arun Kumar, Sir Padam Pat Singhanian University, Udaipur, Rajasthan  
Mr. Muhammad Imran Khan, Universiti Teknologi PETRONAS, Malaysia  
Dr. Natarajan Meghanathan, Jackson State University, Jackson, MS, USA  
Mr. Mohd Zaki Bin Mas'ud, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia  
Prof. Dr. R. Geetharamani, Dept. of Computer Science and Eng., Rajalakshmi Engineering College, India  
Dr. Smita Rajpal, Institute of Technology and Management, Gurgaon, India  
Dr. S. Abdul Khader Jilani, University of Tabuk, Tabuk, Saudi Arabia  
Mr. Syed Jamal Haider Zaidi, Bahria University, Pakistan  
Dr. N. Devarajan, Government College of Technology, Coimbatore, Tamilnadu, INDIA  
Mr. R. Jagadeesh Kannan, RMK Engineering College, India  
Mr. Deo Prakash, Shri Mata Vaishno Devi University, India  
Mr. Mohammad Abu Naser, Dept. of EEE, IUT, Gazipur, Bangladesh  
Assist. Prof. Prasun Ghosal, Bengal Engineering and Science University, India  
Mr. Md. Golam Kaosar, School of Engineering and Science, Victoria University, Melbourne City, Australia  
Mr. R. Mahammad Shafi, Madanapalle Institute of Technology & Science, India  
Dr. F.Sagayaraj Francis, Pondicherry Engineering College, India  
Dr. Ajay Goel, HIET, Kaithal, India  
Mr. Nayak Sunil Kashibarao, Bahirji Smarak Mahavidyalaya, India  
Mr. Suhas J Manangi, Microsoft India  
Dr. Kalyankar N. V., Yeshwant Mahavidyalaya, Nanded, India  
Dr. K.D. Verma, S.V. College of Post graduate studies & Research, India  
Dr. Amjad Rehman, University Technology Malaysia, Malaysia

Mr. Rachit Garg, L K College, Jalandhar, Punjab

Mr. J. William, M.A.M college of Engineering, Trichy, Tamilnadu, India

Prof. Jue-Sam Chou, Nanhua University, College of Science and Technology, Taiwan

Dr. Thorat S.B., Institute of Technology and Management, India

Mr. Ajay Prasad, Sir Padampat Singhania University, Udaipur, India

Dr. Kamaljit I. Lakhtaria, Atmiya Institute of Technology & Science, India

Mr. Syed Rafiul Hussain, Ahsanullah University of Science and Technology, Bangladesh

Mrs Fazeela Tunnisa, Najran University, Kingdom of Saudi Arabia

Mrs Kavita Taneja, Maharishi Markandeshwar University, Haryana, India

Mr. Maniyar Shiraz Ahmed, Najran University, Najran, KSA

Mr. Anand Kumar, AMC Engineering College, Bangalore

Dr. Rakesh Chandra Gangwar, Beant College of Engg. & Tech., Gurdaspur (Punjab) India

Dr. V V Rama Prasad, Sree Vidyanikethan Engineering College, India

Assist. Prof. Neetesh Kumar Gupta, Technocrats Institute of Technology, Bhopal (M.P.), India

Mr. Ashish Seth, Uttar Pradesh Technical University, Lucknow, UP India

Dr. V V S S S Balaram, Sreenidhi Institute of Science and Technology, India

Mr Rahul Bhatia, Lingaya's Institute of Management and Technology, India

Prof. Niranjana Reddy, P, KITS, Warangal, India

Prof. Rakesh. Lingappa, Vijetha Institute of Technology, Bangalore, India

Dr. Mohammed Ali Hussain, Nimra College of Engineering & Technology, Vijayawada, A.P., India

Dr. A.Srinivasan, MNM Jain Engineering College, Rajiv Gandhi Salai, Thorapakkam, Chennai

Mr. Rakesh Kumar, M.M. University, Mullana, Ambala, India

Dr. Lena Khaled, Zarqa Private University, Aman, Jordan

Ms. Supriya Kapoor, Patni/Lingaya's Institute of Management and Tech., India

Dr. Tossapon Boongoen, Aberystwyth University, UK

Dr. Bilal Alatas, Firat University, Turkey

Assist. Prof. Jyoti Praaksh Singh, Academy of Technology, India

Dr. Ritu Soni, GNG College, India

Dr. Mahendra Kumar, Sagar Institute of Research & Technology, Bhopal, India.

Dr. Binod Kumar, Lakshmi Narayan College of Tech.(LNCT) Bhopal India

Dr. Muzhir Shaban Al-Ani, Amman Arab University Amman – Jordan

Dr. T.C. Manjunath, ATRIA Institute of Tech, India

Mr. Muhammad Zakarya, COMSATS Institute of Information Technology (CIIT), Pakistan

Assist. Prof. Harmunish Taneja, M. M. University, India

Dr. Chitra Dhawale, SICSR, Model Colony, Pune, India

Mrs Sankari Muthukaruppan, Nehru Institute of Engineering and Technology, Anna University, India

Mr. Aaqif Afzaal Abbasi, National University Of Sciences And Technology, Islamabad

Prof. Ashutosh Kumar Dubey, Trinity Institute of Technology and Research Bhopal, India

Mr. G. Appasami, Dr. Pauls Engineering College, India

Mr. M Yasin, National University of Science and Tech, Karachi (NUST), Pakistan

Mr. Yaser Miaji, University Utara Malaysia, Malaysia

Mr. Shah Ahsanul Haque, International Islamic University Chittagong (IIUC), Bangladesh

Prof. (Dr) Syed Abdul Sattar, Royal Institute of Technology & Science, India  
Dr. S. Sasikumar, Roever Engineering College  
Assist. Prof. Monit Kapoor, Maharishi Markandeshwar University, India  
Mr. Nwaocha Vivian O, National Open University of Nigeria  
Dr. M. S. Vijaya, GR Govindarajulu School of Applied Computer Technology, India  
Assist. Prof. Chakresh Kumar, Manav Rachna International University, India  
Mr. Kunal Chadha , R&D Software Engineer, Gemalto, Singapore  
Mr. Mueen Uddin, Universiti Teknologi Malaysia, UTM , Malaysia  
Dr. Dhuha Basheer abdullah, Mosul university, Iraq  
Mr. S. Audithan, Annamalai University, India  
Prof. Vijay K Chaudhari, Technocrats Institute of Technology , India  
Associate Prof. Mohd Ilyas Khan, Technocrats Institute of Technology , India  
Dr. Vu Thanh Nguyen, University of Information Technology, HoChiMinh City, VietNam  
Assist. Prof. Anand Sharma, MITS, Lakshmangarh, Sikar, Rajasthan, India  
Prof. T V Narayana Rao, HITAM Engineering college, Hyderabad  
Mr. Deepak Gour, Sir Padampat Singhanian University, India  
Assist. Prof. Amutharaj Joyson, Kalasalingam University, India  
Mr. Ali Balador, Islamic Azad University, Iran  
Mr. Mohit Jain, Maharaja Surajmal Institute of Technology, India  
Mr. Dilip Kumar Sharma, GLA Institute of Technology & Management, India  
Dr. Debojyoti Mitra, Sir padampat Singhanian University, India  
Dr. Ali Dehghantanha, Asia-Pacific University College of Technology and Innovation, Malaysia  
Mr. Zhao Zhang, City University of Hong Kong, China  
Prof. S.P. Setty, A.U. College of Engineering, India  
Prof. Patel Rakeshkumar Kantilal, Sankalchand Patel College of Engineering, India  
Mr. Biswajit Bhowmik, Bengal College of Engineering & Technology, India  
Mr. Manoj Gupta, Apex Institute of Engineering & Technology, India  
Assist. Prof. Ajay Sharma, Raj Kumar Goel Institute Of Technology, India  
Assist. Prof. Ramveer Singh, Raj Kumar Goel Institute of Technology, India  
Dr. Hanan Elazhary, Electronics Research Institute, Egypt  
Dr. Hosam I. Faiq, USM, Malaysia  
Prof. Dipti D. Patil, MAEER's MIT College of Engg. & Tech, Pune, India  
Assist. Prof. Devendra Chack, BCT Kumaon engineering College Dwarahat Almora, India  
Prof. Manpreet Singh, M. M. Engg. College, M. M. University, India  
Assist. Prof. M. Sadiq ali Khan, University of Karachi, Pakistan  
Mr. Prasad S. Halgaonkar, MIT - College of Engineering, Pune, India  
Dr. Imran Ghani, Universiti Teknologi Malaysia, Malaysia  
Prof. Varun Kumar Kakar, Kumaon Engineering College, Dwarahat, India  
Assist. Prof. Nisheeth Joshi, Apaji Institute, Banasthali University, Rajasthan, India  
Associate Prof. Kunwar S. Vaisla, VCT Kumaon Engineering College, India  
Prof Anupam Choudhary, Bhilai School Of Engg.,Bhilai (C.G.),India  
Mr. Divya Prakash Shrivastava, Al Jabal Al garbi University, Zawya, Libya



Associate Prof. Dr. V. Radha, Avinashilingam Deemed university for women, Coimbatore.  
Dr. Kasarapu Ramani, JNT University, Anantapur, India  
Dr. Anuraag Awasthi, Jayoti Vidyapeeth Womens University, India  
Dr. C G Ravichandran, R V S College of Engineering and Technology, India  
Dr. Mohamed A. Deriche, King Fahd University of Petroleum and Minerals, Saudi Arabia  
Mr. Abbas Karimi, Universiti Putra Malaysia, Malaysia  
Mr. Amit Kumar, Jaypee University of Engg. and Tech., India  
Dr. Nikolai Stoianov, Defense Institute, Bulgaria  
Assist. Prof. S. Ranichandra, KSR College of Arts and Science, Tiruchencode  
Mr. T.K.P. Rajagopal, Diamond Horse International Pvt Ltd, India  
Dr. Md. Ekramul Hamid, Rajshahi University, Bangladesh  
Mr. Hemanta Kumar Kalita , TATA Consultancy Services (TCS), India  
Dr. Messaouda Azzouzi, Ziane Achour University of Djelfa, Algeria  
Prof. (Dr.) Juan Jose Martinez Castillo, "Gran Mariscal de Ayacucho" University and Acantelys research Group, Venezuela  
Dr. Jatinderkumar R. Saini, Narmada College of Computer Application, India  
Dr. Babak Bashari Rad, University Technology of Malaysia, Malaysia  
Dr. Nighat Mir, Effat University, Saudi Arabia  
Prof. (Dr.) G.M.Nasira, Sasurie College of Engineering, India  
Mr. Varun Mittal, Gemalto Pte Ltd, Singapore  
Assist. Prof. Mrs P. Banumathi, Kathir College Of Engineering, Coimbatore  
Assist. Prof. Quan Yuan, University of Wisconsin-Stevens Point, US  
Dr. Pranam Paul, Narula Institute of Technology, Agarpara, West Bengal, India  
Assist. Prof. J. Ramkumar, V.L.B Janakiammal college of Arts & Science, India  
Mr. P. Sivakumar, Anna university, Chennai, India  
Mr. Md. Humayun Kabir Biswas, King Khalid University, Kingdom of Saudi Arabia  
Mr. Mayank Singh, J.P. Institute of Engg & Technology, Meerut, India  
HJ. Kamaruzaman Jusoff, Universiti Putra Malaysia  
Mr. Nikhil Patrick Lobo, CADES, India  
Dr. Amit Wason, Rayat-Bahra Institute of Engineering & Boi-Technology, India  
Dr. Rajesh Shrivastava, Govt. Benazir Science & Commerce College, Bhopal, India  
Assist. Prof. Vishal Bharti, DCE, Gurgaon  
Mrs. Sunita Bansal, Birla Institute of Technology & Science, India  
Dr. R. Sudhakar, Dr.Mahalingam college of Engineering and Technology, India  
Dr. Amit Kumar Garg, Shri Mata Vaishno Devi University, Katra(J&K), India  
Assist. Prof. Raj Gaurang Tiwari, AZAD Institute of Engineering and Technology, India  
Mr. Hamed Taherdoost, Tehran, Iran  
Mr. Amin Daneshmand Malayeri, YRC, IAU, Malayer Branch, Iran  
Mr. Shantanu Pal, University of Calcutta, India  
Dr. Terry H. Walcott, E-Promag Consultancy Group, United Kingdom  
Dr. Ezekiel U OKIKE, University of Ibadan, Nigeria  
Mr. P. Mahalingam, Caledonian College of Engineering, Oman

Dr. Mahmoud M. A. Abd Ellatif, Mansoura University, Egypt  
Prof. Kunwar S. Vaisla, BCT Kumaon Engineering College, India  
Prof. Mahesh H. Panchal, Kalol Institute of Technology & Research Centre, India  
Mr. Muhammad Asad, Technical University of Munich, Germany  
Mr. AliReza Shams Shafigh, Azad Islamic university, Iran  
Prof. S. V. Nagaraj, RMK Engineering College, India  
Mr. Ashikali M Hasan, Senior Researcher, CelNet security, India  
Dr. Adnan Shahid Khan, University Technology Malaysia, Malaysia  
Mr. Prakash Gajanan Burade, Nagpur University/ITM college of engg, Nagpur, India  
Dr. Jagdish B. Helonde, Nagpur University/ITM college of engg, Nagpur, India  
Professor, Doctor BOUHORMA Mohammed, University Abdelmalek Essaadi, Morocco  
Mr. K. Thirumalaivasan, Pondicherry Engg. College, India  
Mr. Umbarkar Anantkumar Janardan, Walchand College of Engineering, India  
Mr. Ashish Chaurasia, Gyan Ganga Institute of Technology & Sciences, India  
Mr. Sunil Taneja, Kurukshetra University, India  
Mr. Fauzi Adi Rafrastara, Dian Nuswantoro University, Indonesia  
Dr. Yaduvir Singh, Thapar University, India  
Dr. Ioannis V. Koskosas, University of Western Macedonia, Greece  
Dr. Vasantha Kalyani David, Avinashilingam University for women, Coimbatore  
Dr. Ahmed Mansour Manasrah, Universiti Sains Malaysia, Malaysia  
Miss. Nazanin Sadat Kazazi, University Technology Malaysia, Malaysia  
Mr. Saeed Rasouli Heikalabad, Islamic Azad University - Tabriz Branch, Iran  
Assoc. Prof. Dharendra Mishra, SVKM's NMIMS University, India  
Prof. Shapoor Zarei, UAE Inventors Association, UAE  
Prof. B.Raja Sarath Kumar, Lenora College of Engineering, India  
Dr. Bashir Alam, Jamia millia Islamia, Delhi, India  
Prof. Anant J Umbarkar, Walchand College of Engg., India  
Assist. Prof. B. Bharathi, Sathyabama University, India  
Dr. Fokrul Alom Mazarbhuiya, King Khalid University, Saudi Arabia  
Prof. T.S.Jeyali Laseeth, Anna University of Technology, Tirunelveli, India  
Dr. M. Balraju, Jawahar Lal Nehru Technological University Hyderabad, India  
Dr. Vijayalakshmi M. N., R.V.College of Engineering, Bangalore  
Prof. Walid Moudani, Lebanese University, Lebanon  
Dr. Saurabh Pal, VBS Purvanchal University, Jaunpur, India  
Associate Prof. Suneet Chaudhary, Dehradun Institute of Technology, India  
Associate Prof. Dr. Manuj Darbari, BBD University, India  
Ms. Prema Selvaraj, K.S.R College of Arts and Science, India  
Assist. Prof. Ms.S.Sasikala, KSR College of Arts & Science, India  
Mr. Sukhvinder Singh Deora, NC Institute of Computer Sciences, India  
Dr. Abhay Bansal, Amity School of Engineering & Technology, India  
Ms. Sumita Mishra, Amity School of Engineering and Technology, India  
Professor S. Viswanadha Raju, JNT University Hyderabad, India

Mr. Asghar Shahrzad Khashandarag, Islamic Azad University Tabriz Branch, India  
Mr. Manoj Sharma, Panipat Institute of Engg. & Technology, India  
Mr. Shakeel Ahmed, King Faisal University, Saudi Arabia  
Dr. Mohamed Ali Mahjoub, Institute of Engineer of Monastir, Tunisia  
Mr. Adri Jovin J.J., SriGuru Institute of Technology, India  
Dr. Sukumar Senthilkumar, Universiti Sains Malaysia, Malaysia  
Mr. Rakesh Bharati, Dehradun Institute of Technology Dehradun, India  
Mr. Shervan Fekri Ershad, Shiraz International University, Iran  
Mr. Md. Safiqul Islam, Daffodil International University, Bangladesh  
Mr. Mahmudul Hasan, Daffodil International University, Bangladesh  
Prof. Mandakini Tayade, UIT, RGTU, Bhopal, India  
Ms. Sarla More, UIT, RGTU, Bhopal, India  
Mr. Tushar Hrishikesh Jaware, R.C. Patel Institute of Technology, Shirpur, India  
Ms. C. Divya, Dr G R Damodaran College of Science, Coimbatore, India  
Mr. Fahimuddin Shaik, Annamacharya Institute of Technology & Sciences, India  
Dr. M. N. Giri Prasad, JNTUCE, Pulivendula, A.P., India  
Assist. Prof. Chintan M Bhatt, Charotar University of Science And Technology, India  
Prof. Sahista Machchhar, Marwadi Education Foundation's Group of institutions, India  
Assist. Prof. Navnish Goel, S. D. College Of Enginnering & Technology, India  
Mr. Khaja Kamaluddin, Sirt University, Sirt, Libya  
Mr. Mohammad Zaidul Karim, Daffodil International, Bangladesh  
Mr. M. Vijayakumar, KSR College of Engineering, Tiruchengode, India  
Mr. S. A. Ahsan Rajon, Khulna University, Bangladesh  
Dr. Muhammad Mohsin Nazir, LCW University Lahore, Pakistan  
Mr. Mohammad Asadul Hoque, University of Alabama, USA  
Mr. P.V.Sarathchand, Indur Institute of Engineering and Technology, India  
Mr. Durgesh Samadhiya, Chung Hua University, Taiwan  
Dr Venu Kuthadi, University of Johannesburg, Johannesburg, RSA  
Dr. (Er) Jasvir Singh, Guru Nanak Dev University, Amritsar, Punjab, India  
Mr. Jasmin Cosic, Min. of the Interior of Una-sana canton, B&H, Bosnia and Herzegovina  
Dr S. Rajalakshmi, Botho College, South Africa  
Dr. Mohamed Sarrab, De Montfort University, UK  
Mr. Basappa B. Kodada, Canara Engineering College, India  
Assist. Prof. K. Ramana, Annamacharya Institute of Technology and Sciences, India  
Dr. Ashu Gupta, Apeejay Institute of Management, Jalandhar, India  
Assist. Prof. Shaik Rasool, Shadan College of Engineering & Technology, India  
Assist. Prof. K. Suresh, Annamacharya Institute of Tech & Sci. Rajampet, AP, India  
Dr . G. Singaravel, K.S.R. College of Engineering, India  
Dr B. G. Geetha, K.S.R. College of Engineering, India  
Assist. Prof. Kavita Choudhary, ITM University, Gurgaon  
Dr. Mehrdad Jalali, Azad University, Mashhad, Iran  
Megha Goel, Shamli Institute of Engineering and Technology, Shamli, India

Mr. Chi-Hua Chen, Institute of Information Management, National Chiao-Tung University, Taiwan (R.O.C.)  
Assoc. Prof. A. Rajendran, RVS College of Engineering and Technology, India  
Assist. Prof. S. Jaganathan, RVS College of Engineering and Technology, India  
Assoc. Prof. (Dr.) A S N Chakravarthy, JNTUK University College of Engineering Vizianagaram (State University)  
Assist. Prof. Deepshikha Patel, Technocrat Institute of Technology, India  
Assist. Prof. Maram Balajee, GMRIT, India  
Assist. Prof. Monika Bhatnagar, TIT, India  
Prof. Gaurang Panchal, Charotar University of Science & Technology, India  
Prof. Anand K. Tripathi, Computer Society of India  
Prof. Jyoti Chaudhary, High Performance Computing Research Lab, India  
Assist. Prof. Supriya Raheja, ITM University, India  
Dr. Pankaj Gupta, Microsoft Corporation, U.S.A.  
Assist. Prof. Panchamukesh Chandaka, Hyderabad Institute of Tech. & Management, India  
Prof. Mohan H.S, SJB Institute Of Technology, India  
Mr. Hossein Malekinezhad, Islamic Azad University, Iran  
Mr. Zatin Gupta, Universti Malaysia, Malaysia  
Assist. Prof. Amit Chauhan, Phonics Group of Institutions, India  
Assist. Prof. Ajal A. J., METS School Of Engineering, India  
Mrs. Omowunmi Omobola Adeyemo, University of Ibadan, Nigeria  
Dr. Bharat Bhushan Agarwal, I.F.T.M. University, India  
Md. Nazrul Islam, University of Western Ontario, Canada  
Tushar Kanti, L.N.C.T, Bhopal, India  
Er. Aumreesh Kumar Saxena, SIRTs College Bhopal, India  
Mr. Mohammad Monirul Islam, Daffodil International University, Bangladesh  
Dr. Kashif Nisar, University Utara Malaysia, Malaysia  
Dr. Wei Zheng, Rutgers Univ/ A10 Networks, USA  
Associate Prof. Rituraj Jain, Vyas Institute of Engg & Tech, Jodhpur – Rajasthan  
Assist. Prof. Apoorvi Sood, I.T.M. University, India  
Dr. Kayhan Zrar Ghafoor, University Technology Malaysia, Malaysia  
Mr. Swapnil Sonar, Truba Institute College of Engineering & Technology, Indore, India  
Ms. Yogita Gigras, I.T.M. University, India  
Associate Prof. Neelima Sadineni, Pydha Engineering College, India Pydha Engineering College  
Assist. Prof. K. Deepika Rani, HITAM, Hyderabad  
Ms. Shikha Maheshwari, Jaipur Engineering College & Research Centre, India  
Prof. Dr V S Giridhar Akula, Avanthi's Scientific Tech. & Research Academy, Hyderabad  
Prof. Dr.S.Saravanan, Muthayammal Engineering College, India  
Mr. Mehdi Golsorkhatabar Amiri, Islamic Azad University, Iran  
Prof. Amit Sadanand Savyanavar, MITCOE, Pune, India  
Assist. Prof. P.Oliver Jayaprakash, Anna University, Chennai  
Assist. Prof. Ms. Sujata, ITM University, Gurgaon, India  
Dr. Asoke Nath, St. Xavier's College, India

Mr. Masoud Rafighi, Islamic Azad University, Iran  
Assist. Prof. RamBabu Pemula, NIMRA College of Engineering & Technology, India  
Assist. Prof. Ms Rita Chhikara, ITM University, Gurgaon, India  
Mr. Sandeep Maan, Government Post Graduate College, India  
Prof. Dr. S. Muralidharan, Mepco Schlenk Engineering College, India  
Associate Prof. T.V.Sai Krishna, QIS College of Engineering and Technology, India  
Mr. R. Balu, Bharathiar University, Coimbatore, India  
Assist. Prof. Shekhar. R, Dr.SM College of Engineering, India  
Prof. P. Senthilkumar, Vivekanandha Institute of Engineering And Technology For Woman, India  
Mr. M. Kamarajan, PSNA College of Engineering & Technology, India  
Dr. Angajala Srinivasa Rao, Jawaharlal Nehru Technical University, India  
Assist. Prof. C. Venkatesh, A.I.T.S, Rajampet, India  
Mr. Afshin Rezakhani Roozbahani, Ayatollah Boroujerdi University, Iran  
Mr. Laxmi chand, SCTL, Noida, India  
Dr. Dr. Abdul Hannan, Vivekanand College, Aurangabad  
Prof. Mahesh Panchal, KITRC, Gujarat  
Dr. A. Subramani, K.S.R. College of Engineering, Tiruchengode  
Assist. Prof. Prakash M, Rajalakshmi Engineering College, Chennai, India  
Assist. Prof. Akhilesh K Sharma, Sir Padampat Singhania University, India  
Ms. Varsha Sahni, Guru Nanak Dev Engineering College, Ludhiana, India  
Associate Prof. Trilochan Rout, NM Institute Of Engineering And Technology, India  
Mr. Srikantha Kumar Mohapatra, NMIET, Orissa, India  
Mr. Waqas Haider Bangyal, Iqra University Islamabad, Pakistan  
Dr. S. Vijayaragavan, Christ College of Engineering and Technology, Pondicherry, India  
Prof. Elboukhari Mohamed, University Mohammed First, Oujda, Morocco  
Dr. Muhammad Asif Khan, King Faisal University, Saudi Arabia  
Dr. Nagy Ramadan Darwish Omran, Cairo University, Egypt.  
Assistant Prof. Anand Nayyar, KCL Institute of Management and Technology, India  
Mr. G. Premsankar, Ericsson, India  
Assist. Prof. T. Hemalatha, VELS University, India  
Prof. Tejaswini Apte, University of Pune, India  
Dr. Edmund Ng Giap Weng, Universiti Malaysia Sarawak, Malaysia  
Mr. Mahdi Nouri, Iran University of Science and Technology, Iran  
Associate Prof. S. Asif Hussain, Annamacharya Institute of technology & Sciences, India  
Mrs. Kavita Pabreja, Maharaja Surajmal Institute (an affiliate of GGSIP University), India  
Mr. Vorugunti Chandra Sekhar, DA-IICT, India  
Mr. Muhammad Najmi Ahmad Zabidi, Universiti Teknologi Malaysia, Malaysia  
Dr. Aderemi A. Atayero, Covenant University, Nigeria  
Assist. Prof. Osama Sohaib, Balochistan University of Information Technology, Pakistan  
Assist. Prof. K. Suresh, Annamacharya Institute of Technology and Sciences, India  
Mr. Hassen Mohammed Abdullaah Alsafi, International Islamic University Malaysia (IIUM) Malaysia  
Mr. Robail Yasrab, Virtual University of Pakistan, Pakistan

Mr. R. Balu, Bharathiar University, Coimbatore, India  
Prof. Anand Nayyar, KCL Institute of Management and Technology, Jalandhar  
Assoc. Prof. Vivek S Deshpande, MIT College of Engineering, India  
Prof. K. Saravanan, Anna university Coimbatore, India  
Dr. Ravendra Singh, MJP Rohilkhand University, Bareilly, India  
Mr. V. Mathivanan, IBRA College of Technology, Sultanate of OMAN  
Assoc. Prof. S. Asif Hussain, AITS, India  
Assist. Prof. C. Venkatesh, AITS, India  
Mr. Sami Ulhaq, SZABIST Islamabad, Pakistan  
Dr. B. Justus Rabi, Institute of Science & Technology, India  
Mr. Anuj Kumar Yadav, Dehradun Institute of technology, India  
Mr. Alejandro Mosquera, University of Alicante, Spain  
Assist. Prof. Arjun Singh, Sir Padampat Singhanian University (SPSU), Udaipur, India  
Dr. Smriti Agrawal, JB Institute of Engineering and Technology, Hyderabad  
Assist. Prof. Swathi Sambangi, Visakha Institute of Engineering and Technology, India  
Ms. Prabhjot Kaur, Guru Gobind Singh Indraprastha University, India  
Mrs. Samaher AL-Hothali, Yanbu University College, Saudi Arabia  
Prof. Rajneeshkaur Bedi, MIT College of Engineering, Pune, India  
Mr. Hassen Mohammed Abdullah Alsafi, International Islamic University Malaysia (IIUM)  
Dr. Wei Zhang, Amazon.com, Seattle, WA, USA  
Mr. B. Santhosh Kumar, C S I College of Engineering, Tamil Nadu  
Dr. K. Reji Kumar, , N S S College, Pandalam, India  
Assoc. Prof. K. Seshadri Sastry, EIILM University, India  
Mr. Kai Pan, UNC Charlotte, USA  
Mr. Ruikar Sachin, SGGSIET, India  
Prof. (Dr.) Vinodani Katiyar, Sri Ramswaroop Memorial University, India  
Assoc. Prof., M. Giri, Sreenivasa Institute of Technology and Management Studies, India  
Assoc. Prof. Labib Francis Gergis, Misr Academy for Engineering and Technology (MET), Egypt  
Assist. Prof. Amanpreet Kaur, ITM University, India  
Assist. Prof. Anand Singh Rajawat, Shri Vaishnav Institute of Technology & Science, Indore  
Mrs. Hadeel Saleh Haj Aliwi, Universiti Sains Malaysia (USM), Malaysia  
Dr. Abhay Bansal, Amity University, India  
Dr. Mohammad A. Mezher, Fahad Bin Sultan University, KSA  
Assist. Prof. Nidhi Arora, M.C.A. Institute, India  
Prof. Dr. P. Suresh, Karpagam College of Engineering, Coimbatore, India  
Dr. Kannan Balasubramanian, Mepco Schlenk Engineering College, India  
Dr. S. Sankara Gomathi, Panimalar Engineering college, India  
Prof. Anil kumar Suthar, Gujarat Technological University, L.C. Institute of Technology, India  
Assist. Prof. R. Hubert Rajan, NOORUL ISLAM UNIVERSITY, India  
Assist. Prof. Dr. Jyoti Mahajan, College of Engineering & Technology  
Assist. Prof. Homam Reda El-Taj, College of Network Engineering, Saudi Arabia & Malaysia  
Mr. Bijan Paul, Shahjalal University of Science & Technology, Bangladesh

Assoc. Prof. Dr. Ch V Phani Krishna, KL University, India  
Dr. Vishal Bhatnagar, Ambedkar Institute of Advanced Communication Technologies & Research, India  
Dr. Lamri LAOUAMER, Al Qassim University, Dept. Info. Systems & European University of Brittany, Dept.  
Computer Science, UBO, Brest, France  
Prof. Ashish Babanrao Sasankar, G.H.Raisoni Institute Of Information Technology, India  
Prof. Pawan Kumar Goel, Shamli Institute of Engineering and Technology, India  
Mr. Ram Kumar Singh, S.V Subharti University, India  
Assistant Prof. Sunish Kumar O S, Amaljiyothi College of Engineering, India  
Dr Sanjay Bhargava, Banasthali University, India  
Mr. Pankaj S. Kulkarni, AVEW's Shatabdi Institute of Technology, India  
Mr. Roohollah Etemadi, Islamic Azad University, Iran  
Mr. Oloruntoyin Sefiu Taiwo, Emmanuel Alayande College Of Education, Nigeria  
Mr. Sumit Goyal, National Dairy Research Institute, India  
Mr Jaswinder Singh Dilawari, Geeta Engineering College, India  
Prof. Raghuraj Singh, Harcourt Butler Technological Institute, Kanpur  
Dr. S.K. Mahendran, Anna University, Chennai, India  
Dr. Amit Wason, Hindustan Institute of Technology & Management, Punjab  
Dr. Ashu Gupta, Apeejay Institute of Management, India  
Assist. Prof. D. Asir Antony Gnana Singh, M.I.E.T Engineering College, India  
Mrs Mina Farmanbar, Eastern Mediterranean University, Famagusta, North Cyprus  
Mr. Maram Balajee, GMR Institute of Technology, India  
Mr. Moiz S. Ansari, Isra University, Hyderabad, Pakistan  
Mr. Adebayo, Olawale Surajudeen, Federal University of Technology Minna, Nigeria  
Mr. Jasvir Singh, University College Of Engg., India  
Mr. Vivek Tiwari, MANIT, Bhopal, India  
Assoc. Prof. R. Navaneethakrishnan, Bharathiyar College of Engineering and Technology, India  
Mr. Somdip Dey, St. Xavier's College, Kolkata, India  
Mr. Souleymane Balla-Arabé, Xi'an University of Electronic Science and Technology, China  
Mr. Mahabub Alam, Rajshahi University of Engineering and Technology, Bangladesh  
Mr. Sathyapraksh P., S.K.P Engineering College, India  
Dr. N. Karthikeyan, SNS College of Engineering, Anna University, India  
Dr. Binod Kumar, JSPM's, Jayawant Technical Campus, Pune, India  
Assoc. Prof. Dinesh Goyal, Suresh Gyan Vihar University, India  
Mr. Md. Abdul Ahad, K L University, India  
Mr. Vikas Bajpai, The LNM IIT, India  
Dr. Manish Kumar Anand, Salesforce (R & D Analytics), San Francisco, USA  
Assist. Prof. Dheeraj Murari, Kumaon Engineering College, India  
Assoc. Prof. Dr. A. Muthukumaravel, VELS University, Chennai  
Mr. A. Siles Balasingh, St. Joseph University in Tanzania, Tanzania  
Mr. Ravindra Daga Badgujar, R C Patel Institute of Technology, India  
Dr. Preeti Khanna, SVKM's NMIMS, School of Business Management, India  
Mr. Kumar Dayanand, Cambridge Institute of Technology, India

Dr. Syed Asif Ali, SMI University Karachi, Pakistan

Prof. Pallvi Pandit, Himachal Pradesh University, India

Mr. Ricardo Verschueren, University of Gloucestershire, UK

Assist. Prof. Mamta Juneja, University Institute of Engineering and Technology, Panjab University, India

Assoc. Prof. P. Surendra Varma, NRI Institute of Technology, JNTU Kakinada, India

Assist. Prof. Gaurav Shrivastava, RGPV / SVITS Indore, India

Dr. S. Sumathi, Anna University, India

Assist. Prof. Ankita M. Kapadia, Charotar University of Science and Technology, India

Mr. Deepak Kumar, Indian Institute of Technology (BHU), India

Dr. Dr. Rajan Gupta, GGSIP University, New Delhi, India

Assist. Prof M. Anand Kumar, Karpagam University, Coimbatore, India

Mr. Mr Arshad Mansoor, Pakistan Aeronautical Complex

Mr. Kapil Kumar Gupta, Ansal Institute of Technology and Management, India

Dr. Neeraj Tomer, SINE International Institute of Technology, Jaipur, India

Assist. Prof. Trunal J. Patel, C.G.Patel Institute of Technology, Uka Tarsadia University, Bardoli, Surat

Mr. Sivakumar, Codework solutions, India

Mr. Mohammad Sadegh Mirzaei, PGNR Compnay, Iran

Dr. Gerard G. Dumancas, Oklahoma Medical Research Foundation, USA



# **CALL FOR PAPERS**

## **International Journal of Computer Science and Information Security**

**IJCSIS 2013**

**ISSN: 1947-5500**

**<http://sites.google.com/site/ijcsis/>**

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

### ***Track A: Security***

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity

Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc.), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on

its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

### ***Track B: Computer Science***

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embedded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC's, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration : Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail [ijcsiseditor@gmail.com](mailto:ijcsiseditor@gmail.com). Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at <http://sites.google.com/site/ijcsis/authors-notes> .



**© IJCSIS PUBLICATION 2013**

**ISSN 1947 5500**

**<http://sites.google.com/site/ijcsis/>**